

MONOGRAFÍA “CARACTERÍSTICAS Y PARÁMETROS DE LA SEGURIDAD EN LA TRANSMISIÓN DE DATOS PARA LOS DISPOSITIVOS SMART TV”

JOHANA ROCIO ROJAS CAMACHO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA, E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
LIBANO TOLIMA
2018**

**MONOGRAFÍA “CARACTERÍSTICAS Y PARÁMETROS DE LA SEGURIDAD
EN LA TRANSMISIÓN DE DATOS PARA LOS DISPOSITIVOS SMART TV”**

**JOHANA ROCIO ROJAS
CAMACHO**

**Monografía de para optar el título de Especialista en Seguridad
Informática**

**Director
ING. FRANCISCO JAVIER HILARION NOVOA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA, E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
LIBANO TOLIMA
2018**

Nota de aceptación

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, Octubre de 2018

DEDICATORIA

Este trabajo es dedicado con mi sentimiento a mi hija y mi esposo, por ser incondicionales, por darme la oportunidad de educarme, su apoyo es la base, de un logro cumplido orgullo de todos, el resultado de este proyecto representa la culminación de una etapa educativa. Gracias.

CONTENIDO

1.	RESUMEN.....	11
2.	INTRODUCCION	13
3.	TITULO	15
4.	DEFINICION DEL PROBLEMA.....	16
4.1.	ANTECEDENTES DEL PRLOBLEMA	16
4.2.	FORMULACION DEL PROBLEMA	17
4.3.	DESCRIPCION DEL PROBLEMA	17
5.	JUSTIFICACION.....	19
6.	OBJETIVOS.....	21
6.1.	OBJETIVO GENERAL.....	21
6.2.	OBJETIVOS ESPECIFICOS	21
7.	MARCO DE REFERENCIA.....	22
7.1.	MARCO TEORICO.....	22
7.1.1.	¿Qué es un Smart TV?	22
7.1.2.	Señal del Televisión.....	22
7.2.	MARCO CONCEPTUAL.....	31
7.2.1.	Seguridad Informática.....	31
7.2.2.	Vulnerabilidades	34
7.2.3.	Amenazas.....	36

7.3. CÓMO ACTUAR.....	37
7.3.1. Delitos.....	38
7.4. MARCO LEGAL.....	42
8. ESQUEMA TEMATICO.....	46
8.1. CAPITULO I SMART TV.....	46
8.1.1. Historia	47
8.1.2. Evolución	50
8.1.3. Futuro	55
8.2. CAPITULO I CARACTERISTICAS Y PARAMETROS DE SEGURIDAD EN LA TRASMISION DE DATOS PARA LOS SMART TV	57
8.2.1. Proveedores	59
8.2.2. Arquitectura	59
8.2.3. Vulnerabilidades en la seguridad de los Smart TV	71
8.3. CAPITULO II ATAQUES, ERRORES Y MEDIDAS DE SEGURIDAD EN LOS SMART TV	75
8.3.1. Ataques más comunes a los dispositivos Smart TV	77
8.3.2. Errores de los usuarios	82
8.3.3. Aplicaciones seguras para los Smart TV	87
8.4. CAPITULO III CARACTERISTICAS DE LA SEGURIDAD DE LOS SISTEMAS OPERATIVOS USADOS EN LOS SMART TV	91

9. CONCLUSIONES	97
BIBLIOGRAFIA.....	99
ANEXOS	102

LISTA DE FIGURAS

	Pag.
Figura 1 Evolución de la Televisión.....	51
Figura 2 Evolución de la Televisión 2.....	52
Figura 3 Evolución de la Televisión 3.....	52
Figura 4 Evolución de la Televisión 4.....	53
Figura 5 Evolución de la Televisión 5.....	54
Figura 6 Smart TV	58
Figura 7 Aplicaciones de los Smart TV	60

LISTA DE TABLAS

	Pag.
Tabla 1 Clasificación de las vulnerabilidades	36
Tabla 2 Sistemas Operativos	61

LISTA DE ANEXOS

	Pag.
Anexo A Formato RAE.....	102

1. RESUMEN

Con el desarrollo de la presente monografía se pretende promover la seguridad de las nuevas tecnologías, en este caso los dispositivos Smart TV, esta es una propuesta que aborda el tema de seguridad de la información en dispositivos que captan la atención de la mayoría de los usuarios que hacen uso de este dispositivo.

La adquisición de la tecnología Smart viene en aumento, según la Revista Diners de Marzo de 2016 en un artículo que titula ¿Cómo está cambiando la forma de ver televisión en los Smart TV?, describe básicamente el condicionamiento de la forma de vida y la conectividad casi que las 24 horas del día a la internet, permitiendo así que el usuario este hiperconectado mediante una pantalla, esta crea dependencia por la variedad de las aplicaciones y novedades que presentan los Sistemas Operativos en este caso los usados son Android TV, Tizen, Firefox OS o WebOs, los cuales buscan generar mejores experiencias en su uso.

Mediante una consultoría de Future Source en el planeta hay más de mil millones de Televisores con estas características y según los datos del DANE en Colombia, existen 14 millones de aparatos frente a 13 millones de familias y en promedio cada colombiano esta dos horas diarias frente al televisor, aparte que el televisor no tiene un único dueño, sino que corresponde al hogar, aunque la utilización de este tipo de dispositivos es convencional, simplemente sentarse a divisar contenido televisor,

una buena parte de esta población utiliza esta tecnología para manipular información importante, datos, imágenes, video, transacciones de dinero, en fin, todo lo que tiene que ver con información, datos personales; de igual forma el aumento de las amenazas y riesgos, accesos indeseables a este tipo de operaciones, intersecciones en las comunicaciones, es preocupante, ya que no existe un método en donde la información este protegida en un 100%.

Con lo citado se quiere fortalecer el conocimiento en cuanto a vulnerabilidades y fortalezas de la información en los Smart TV, desde la perspectiva de un currículo de Especialista en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD.

2. INTRODUCCION

La forma como la tecnología avanza cada día y la manera de hacer uso de la información desde el nuevo siglo ha tomado un papel muy importante para los usuarios, la tecnología avanza cada día a pasos agigantados, actualmente los usuarios se adaptan de una manera fácil a cada producto tecnológico, herramientas básicas que fortalecen procesos que se ejecutan por medio de la misma, estos se han visto en la necesidad de adaptarse y sistematizar su información por medio de sistemas de información que a su vez se encuentran en computadores hiperconectados, esto significa que tiene acceso a internet, de igual forma los ataques a la información y las personas que hacen mal uso de su conocimiento quieren hacer mal uso de la información, lo que puede llevar a daño en la misma, perdida etc. las consecuencias son complejidad de problemas, ya que en la actualidad la información se ha convertido en uno de los activos más importantes de usuarios y de las organizaciones, al verse afectada puede causar daños económicos muy grandes. La falta de conocimiento, cultura en seguridad informática, educación tecnológica, el poco entendimiento, la baja inversión presupuestal en educación sobre este tipo de temas son los motivos principales para generar controversia, dejar la ignorancia tecnológica que en la actualidad debería de ser un aspecto importante presente a la hora de hacer uso de la tecnología.

Debido a lo anterior, se realizará un análisis e identificación del estado actual de la seguridad informática de los dispositivos Smart TV, y estará enfocado en la revisión de la literatura respecto vulnerabilidades y actuaciones de usuarios que no conocen medidas básicas de protección de datos, al igual sobre el debido manejo que se le debe dar a su información personal, de esta forma permitirá brindar un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información.

3. TITULO

CARACTERÍSTICAS Y PARÁMETROS DE LA SEGURIDAD EN LA
TRANSMISIÓN DE DATOS PARA LOS DISPOSITIVOS SMART TV.

4. DEFINICION DEL PROBLEMA

4.1. ANTECEDENTES DEL PRLOBLEMA

Con el auge de la tecnología, las conexiones a internet y la dependencia que actualmente los usuarios crean ante este tipo de dispositivos, en este caso los Smart TV, la mayoría de las personas quieren estar a la vanguardia, no quedarse de utilizar y conocer este mundo que en cierta media ofrece un sin número de beneficios y al mismo tiempo hace que la información sea vulnerable a una gran cantidad de personas mal intencionadas que en ocasiones logran robar información valiosa de los usuarios. La transmisión de información entre los dispositivos Smart TV, necesita de una metodología en dichas emisiones de tal forma que permitan un nivel aceptable de seguridad.

Teniendo en cuenta lo anterior, nace la necesidad de identificar cuáles son los ataques más comunes, las operaciones que el usuario realiza que puedan presentar vulnerabilidades, clasificación puede permitir la identificación de errores de los usuarios cuando hacen uso de este tipo de dispositivos. Lo que busca el desarrollo de la monografía es determinar las características y parámetros de la seguridad para los Smart TV.

4.2. FORMULACION DEL PROBLEMA

¿Cómo se puede proteger la información personal de los usuarios comunes que es administrada por dispositivos Smart TV garantizando confidencialidad, disponibilidad e integridad de los datos?

4.3. DESCRIPCION DEL PROBLEMA

La seguridad informática tiene un papel muy importante, teniendo en cuenta que la información es el activo protagonista, por tal razón debe considerarse la importancia de protegerla, esta puede ser encontrada de distintas formas ya sea que este almacenada electrónicamente, a través de correos electrónicos, videos, grabaciones, fotos, datos o en cualquier medio digital etc. Es así que a través de cualquiera de estos medios la información se puede ver afectada.

En la antigüedad la seguridad principalmente era física ya que la mayoría de la información se encontraba en papel, pero en la actualidad la prioridad está en el soporte informático y la seguridad lógica. Los delitos informáticos han tenido un gran aumento a nivel mundial, la falta de conocimiento sobre cómo deben protegerse de estos delitos es casi que nula, los usuarios solo quieren navegar, ir y venir en el ciberespacio, nunca se detienen a pensar en un salvavidas para la información o en un medio de protección; no sería necesario proteger la información si no existiera quien la necesite o quien pague por conseguirla, es por esto que se debe tener en

cuenta el mercado negro de la información, la cual busca obtener bases de datos con información personal para distintos fines.

En la actualidad existen varias técnicas en donde personas logran obtener información secreta, esto conlleva a costosas pérdidas económicas, legales o incluso la imagen personal de los usuarios, es allí donde se ve la necesidad de derribar algunos mitos y aclarar algunos conceptos sobre la importancia de la seguridad de la información al momento de hacer uso de los dispositivos Smart TV. Ahora la descripción es más clara, el generar conciencia de que todos tenemos algo que ver en el manejo de esta, el planteamiento consiste en analizar e identificar el estado actual de la seguridad información en los dispositivos Smart TV, usuarios de la vida cotidiana, el cual brindara una formula general sobre la importancia y medidas necesarias para proteger los datos en el activo, con el fin de contextualizarnos e identificar en que radica esa importancia y adquirir conocimiento de los pasos y prevenciones que se deben tomar a la hora de hacer uso de la información en este tipo de dispositivos.

5. JUSTIFICACION

La tecnología día a día trae algo nuevo, atractivo, la mayoría de los usuarios quieren acceder a un mundo sin fronteras, una característica fundamental es que al momento de tener un dispositivo tecnológico en su mayoría y todo lo que encontramos aquí es información, este es el principal protagonista, pero al mismo tiempo no se le da un debido manejo por tal razón lo que se quiere es Identificar los factores o amenazas que ponen en riesgo la seguridad de la información que fluye a través de dispositivos en este caso los Smart TV en usuarios domésticos, para proponer un desarrollo su conocimiento, en donde se aprenda a hacer uso de normas, pautas en donde se maneje la información de forma prudente y a su vez se proteja, que sea vista desde el punto de que esta es única e intransferible. Al tener conocimiento de las características normas de seguridad que se deben tener con la información, los usuarios estarían adquiriendo conocimiento y dando un valor agregado al uso de este tipo de dispositivos.

Gracias al aumento de adquisición de estos dispositivos y al acceso a internet que permite este tipo de tecnología, la cantidad de transmisiones en cuanto a datos, voz, video, archivos aumentan, a partir de distintos casos de éxito sobre proyectos de seguridad informática, se puede demostrar que el uso de buenas prácticas y conocimiento en seguridad informática permite garantizar la correcta administración

de los riesgos a partir de la identificación de las características y parámetros de seguridad que se empleen en los dispositivos Smart TV.

6. OBJETIVOS

6.1. OBJETIVO GENERAL

Desarrollar una monografía que condense las principales características y parámetros de seguridad en transmisión de datos para los Smart TV teniendo en cuenta diferentes Sistemas Operativos.

6.2. OBJETIVOS ESPECIFICOS

- Realizar un Análisis de la evolución de los dispositivos Smart TV.
- Determinar parámetros y características de seguridad de los sistemas operativos más comunes en los dispositivos Smart TV.
- Identificar los errores más comunes que comenten los usuarios durante su uso y herramientas que permitan mejorar la seguridad de la información en dispositivos Smart TV.
- Determinar cuáles son los Sistemas Operativos más recomendables que permitan salvaguardar la información en los dispositivos Smart TV.

7. MARCO DE REFERENCIA

7.1. MARCO TEORICO

7.1.1. ¿Qué es un Smart TV?

Televisor con tecnología avanzada, inteligente, su característica principal es la conexión a internet y el sin número de beneficios que contiene, uno de ellos es la comunicación entre dispositivos con conexión a internet tablets, teléfonos, relojes inteligentes entre otros. Con el objetivo de proporcionar interactividad y otras características avanzadas que no ofrece la televisión tradicional.

7.1.2. Señal del Televisión

Televisión digital terrestre

Teniendo en cuenta TELEVISION DIGITAL. Es una forma novedosa de ver contenidos en la televisión gracias a las nuevas tecnologías de los medios digitales la cual permite transmitir contenidos por medio de una antena aérea convencional. La tecnología con este tipo de características hace que aumente el número de canales añadido a esto calidad en imagen y el sonido. Haciendo referencia al párrafo de TELEVISION DIGITAL TERRSTRE¹, esta es una de las medios más usada en centro América países como EEUU, Canadá, Honduras, El Salvador y México, Asia con el nombre de ATSC, ISDB-T, en Japón y Filipinas con el nombre de ISDB-Tb variante del ISDB-T, en Latinoamérica países como Argentina, Perú

Nicaragua, Bolivia, Uruguay, Paraguay, Chile, Ecuador, Venezuela, , Costa Rica y Guatemala, a excepción de Colombia, Guyana, Panamá, Honduras, Surinamés, México y el Salvador, DTMB en la República Popular China, Macau y Hong Kong, DVB-T en los países europeos, Australia, partes de África. El resto del mundo aún no se ha decidido. ¹

La TDT admite que la calidad de la llegada de la señal número disponible de canales al igual que la versatilidad del sistema teniendo en cuenta sonido multicanal, varias señales de audio, close capitón, guía de canales y programación, canales de emisoras, servicios participativos, imagen panorámica, etc. Teniendo en cuenta estas características la TV análoga desaparecerá en un 100%, liberando frecuencias que permitirán ofrecer canales con alta calidad y otros servicios en TDT.

Televisión digital por cable

Tipo de señal que se trasmite por medio de sistemas de TV por clave este tipo puede ser Coaxial o telefónico. En Latinoamérica el principal operador de este tipo de servicios es Telmex y Claro TV.

Haciendo una comparación con países Europeos TELEVISION DIGITAL Y TIPOS DE SEÑALES ² España en este caso AUNA y ONO son las principales plataformas

¹ 1 TELEVISION DIGITAL, {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en: https://es.wikipedia.org/wiki/Televisi%C3%B3n_digital

que emitían televisión digital por cable, AUNA y ONO, permitieron que se digitalizara en 2005 tenía digitalizado el 58% y AUNA el 90% de su red, actualmente el grupo de cable gallego "R" está convirtiendo su cabecera en digital por lo que próximamente dará el servicio de televisión digital además de ofrecer los canales gratuitos de la TDT.²

IPTV Protocolo de televisión IP

En Europa enfocado en el país de España principalmente, la TV por banda ancha es novedosa. Movistar realizó un proyecto llamado Imagenio o Movistar TV el cual brinda a sus usuarios un paquete denominado Tripe Play o trío, el cual contiene televisión digital, permite contenidos de internet por medio banda ancha y voz haciendo uso del protocolo IP (VoIP). En 2006, Movistar TV logró un margen de 206.572 clientes y proyecta que para los siguientes años esta cifra sea superada en 100% de usuarios.

Como lo indica Estrategias de Mercado por Internet ³, lo que ofrece este paquete es que el medio donde se transmite que es un par de cobre de hilo telefónico, permita afianzar medio para recibir canales de tv, vídeo a la orden, espectáculos o películas repagadas algo ya conocido como, Pay Per View en Inglés. Los avances en la tecnología de los sistemas ADSL, hacen que exista mejor y mayor velocidad de conexión en la transmisión de numerosos canales, aparte de interactividad con otros

² TELEVISION DIGITAL, TIPOS DE SENALES. {En línea}. {Consultado el 22 de Febrero de 2018}
Disponible en: <https://sites.google.com/site/historiadetv/television-digital/tipos-de-senales>

usuarios, demostraciones certeras para que las compañías de televisión por ADSL permitan que los métodos de difusión sean más económicos que el cable coaxial ya que se aprovecha la infraestructura telefónica existente.³

Televisión digital por satélite

Apreciando televisión digital, tipos de señales⁴. Los conceptos estarían denotados en todas las transmisiones de señal satelital de forma digital. Sus principales proveedores en el globo terráqueo son Telmex, Sky, DirecTV, Telefónica, Claro y VTR.

Estos son los formatos que más usuarios agrupan en la televisión por suscripción, a pesar de que ha decaído las plataformas Digital y Canal Satélite Digital ha pasado de transmisiones grabadas a eventos en línea o transmisiones online, es así que se ha fusionado creando Digital. Donde sus mayores ingresos se derivan de la transmisión en directo de diferentes contenidos como deportes, reality 's, programas de juego entre otros.

Televisión analógica

La televisión analógica es un servicio que ofrece un método acostumbrado de televisión, el cual hace uso de señales electromagnéticas para transferir y dar a conocer imágenes y sonidos. Este sistema se usa desde la apertura de las emisiones de televisión, con una historia de más de 50 años. Un gran número de

³ ESTRATEGIAS DE MERCADO POR INTERNET. {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en: http://www.icesi.edu.co/blogs_estudiantes/juanmartin/2009/04/25/television-digital/

países encuentran en un período de transmisión forma en mejorar el tipo de señal y unirse a la nueva era de la tecnología en este caso el tipo de señal que se implementara a los usuarios que permanecen a la vanguardia de sumergirse en este mundo atractivo, en el que coexisten tanto emisiones en analógico como en digital.

TV digital vs. Tv analógica

Uno de los principales inconvenientes de la televisión analógica es que se quedó rezagada en los contenidos convencionales, las señales de vídeo no son atractivas cambian poco al pasar de un elemento de imagen (píxel) a los contiguos, en pocas palabras, se malgasta espectro electromagnético, otro aspecto son el número de canales que transmiten contenidos similares y la interferencia que se convierte en un problema grave. La televisión analógica, la imagen y del sonido se presentan por las magnitudes analógicas de una señal eléctrica la cual ocupa muchos recursos en su transmisión. ⁴

De acuerdo con TELEVISION DIGITAL, TIPOS DE SENALES ⁵. La transmisión de la señal digital está representada en base dos por números, los dígitos “1” y “0”. Es un proceso de conversión en donde la señal se representa de forma numérica en bits, esto permite que la señal sea sometida a procesos complejos como, excelente calidad en la señal, la cual permite la conexión y la operación de varios procesos en

⁴ TELEVISION DIGITAL, TIPOS DE SENALES. {En línea}. {Consultado el 22 de Febrero de 2018}
Disponible en: <https://sites.google.com/site/historiadetv/>

los hogares que se trasmite este tipo de señales. Actuando de manera simultánea hay que tener presente que, las señales digitales que se ofrecen de forma directa por medio de un conversor analógico-digital, permiten el pago de gran cantidad de bits lo cual hace que no sea posible el transporte y aceptación sin un consumo excesivo de recursos.

El agrupamiento de la señal en bits hace que el proceso de digitalizar la señal de TV sea alta, lo cual estaría necesitando alto grado de almacenamiento y de recurso para su transporte. A continuación, se presentan una serie de características que presentan los diferentes formatos de Televisión los cuales generan digitalización.

- **Formato Convencional (4:3)** imagen digital de TV está formada por 720x576 puntos pixeles. Almacena una imagen requiere: 1 Mbyte. Transmite un segundo de imágenes continuas, requiere una velocidad de transmisión de 170 Mbits/s.
- **Formato Panorámico (16:9)** una imagen digital de televisión está formada por 960x 576 puntos pixeles. Requiere un 30% más de capacidad que el formato 4:3
- **Formato de Alta definición** la imagen digital de televisión consiste en 1920 x1080 puntos pixeles. Almacena una imagen requiere más de 4Mbyte por imagen. Hace una transmisión de un segundo de imágenes continuas, requiere gran velocidad de transmisión de 1Gbit/s. Las señales de televisión tienen mucha más información que la que el ojo humano necesita para

observar correctamente una imagen. Es decir, tienen una abundancia considerable.⁵

Esta abundancia es explotada por las numerosas técnicas digitales, las cuales permiten reducir la cantidad de "números" generados en la digitalización hasta niveles propios que dan paso al envío de la señal con alto grado de calidad y recursos, este método de transporte de señal digital entre otras, permiten que factores que han impulsado definitivamente el desarrollo de la televisión Digital, aumenten el almacenamiento y envío de la señal de televisión digital con mínimo uso de recursos.

De acuerdo con Televisión digital⁶, los canales radioeléctricos de la televisión digital necesitan la gran mayoría de recursos o el mismo espacio de banda (8MHz) a cambio de los canales utilizados por la televisión analógica, esto genera la utilización de técnicas de compresión, que quiere decir que la señal con imagen y sonido (MPEG), poseen la capacidad de generar una variable en programas de quiere decir que cuando la televisión emplea la velocidad de transmisión, reconoce variaciones entre un único programa de televisión de alta definición (alta calidad de imagen y sonido) a cinco programas con calidad técnica similar a la actual (norma de emisión G con sistema de color PAL), también permite incluir más programas con calidad similar al vídeo. Aunque no es propio, inicialmente, se ha previsto que

⁵ TELEVISION DIGITAL, TIPOS DE SENALES. {En línea}. {Consultado el 22 de Febrero de 2018}
Disponible en: <http://www.electrohogar.net/descargas/TDT.pdf>

cada canal múltiple (canal múltiple se refiere a las características que posee para de que un canal albergue muchos programas de televisión) con una acogida a nivel nacional o autonómica, haciendo uso como mínimo cuatro programas. ⁶

Visión General

De acuerdo con el artículo de la comunicación de regulación de comunicaciones, al Hablar de televisores inteligentes se refiere en una parte exclusiva a un televisor que cuenta con conexión a internet, se puede referir en un término más amplio a tecnología moderna con mayor conectividad que se sale de un concepto de televisión donde solo se proyectaban escenas por medio de señal análoga, estos a su vez tienen grandes características como instalación y ejecución de aplicaciones avanzadas como Plugins, divisar contenidos en línea video, fotos, películas y música, mediante IPTV (*Internet Protocolo Televisión*) navegar buscar por internet, personalizar contenidos, tener acceso a redes sociales y un sin número de aplicaciones de multimedia, ver contenidos de alta definición, participar en sistemas de votaciones online, juegos y participación en concursos(*publicidad interactiva*). ⁷

Teniendo en cuenta el contenido de la página que es un Smart TV Características, tener acceso a los contenidos copiándolos en discos personales, hacer

⁶ TELEVISION DIGITAL. {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en: <https://www.monografias.com/trabajos5/tv/tv.shtml>

⁷ QUE ES SMART TV CARACTERISTICAS. {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en: Diagnostico TV _ CRC_23_03_2011 para publicacion_sin_cc.pdf

reproducciones en línea de música y video, permitir tener acceso a aplicaciones como juegos, compras en línea, sincronizar el teléfono personal con el televisor.

Teniendo en cuenta un artículo Android o ISO y como básicamente los diseñadores de los Sistemas Operativos de Celulares trabajan para el diseño del sistema Operativos de televisores se da la siguiente opinión, el tipo de medios que tienen estos privilegios son Sistema Android e iPhone, aparte que algunas de estas máquinas permiten hacer llamadas online mediante Skype, su sistema operativo está diseñado bajo una plataforma de Software libre y en su mayoría el sistema más utilizado es el Androide el cual se basa en actualización automáticas activada mediante una conexión a internet.

El sistema operativo SO en su mayoría para este tipo de televisores está basado en una plataforma de código abierto y el sistema más utilizado es el Androide y se actualiza desde el propio dispositivo utilizando una conexión a internet o Ethernet ya que cuenta con este tipo de conexión que se dirige a conexiones de modem de banda ancha o Router, generalmente y la conexión más usada es la conexión inalámbrica o Wifi.

La experiencia para los usuarios es optimiza todos los medios de comunicación lo cual casi que genera perfección para accesibilidad a EPG (*Guía electrónica de Programas*) permite conexión de teclados y mousse genéricos ya que cuenta con

una interfaz que como la mayoría se maneja de manera intuitiva y cómoda, y algunos responden a órdenes de voz y movimiento.

Integra sintonizados TDT, también puerto HDMI además de salidas RCA. Todos los televisores Smart TV cuentan con fabricantes de accesorios para reproducir videos en alta definición 2d o 3d, para adquirir mayor sensación y profundidad en su servicio.⁸

7.2. MARCO CONCEPTUAL

7.2.1. Seguridad Informática

Según el artículo de Seguridad Informática⁹, La seguridad informática, es conocida como ciberseguridad o seguridad de tecnologías de la información, área relacionada la tecnología. Se enfoca mantener a la vanguardia la infraestructura computacional y todo lo que tenga que ver con este, especialmente, la información que contenga en una computadora o que viaje a través de las redes de los ordenadores.

Actualmente existen varios estándares, protocolos, métodos, reglas, herramientas y leyes la cuales permiten minimizar futuros riesgos a los medios que contienen los

⁸ QUE ES SMART TV CARACTERISTICAS. {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en:

https://www.bbc.com/mundo/noticias/2015/10/151014_android_ios_celulares_seguros_jm

⁹ SEGURIDAD INFORMATICA. {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

datos o de la información. La ciberseguridad alcanza niveles de software (bases de datos, metadatos, archivos), hardware, redes de ordenadores y todo lo que para las compañías signifique algún tipo de riesgo, si esta información intima la obtienen personas ajenas, se estaría llegando a niveles preocupantes ya que es para muchas es la base principal del negocio. El concepto de seguridad de la información no se debe ser confundir con el de seguridad informática, el objetivo principal de la última es solo asegurar el medio informático, pero la información puede encontrarse en diferentes medios y formas, y no solo en medios informáticos. La seguridad informática son métodos que se encarga de diseñar las normas, procedimientos, métodos y técnicas los cuales logran que un sistema de información seguro y confiable.

La seguridad en un ambiente de red es la habilidad que se adquiere para identificar y eliminar vulnerabilidades. La definición de seguridad se debe también a la intención de salvaguardar las ventajas de las organizaciones teniendo en cuenta todos los aspectos como dispositivos físicos, computadores. Ningún individuo a cargo de seguridad debe determinar quién y cuándo puede tomar acciones determinadas sobre un ítem en específico. Cuando se trata de la seguridad de la información de una compañía, lo fundamental varía de organización en organización. Indiferente, cualquier organización con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación ⁹.

Objetivos

Según la página de seguridad informática ¹⁰, los medios con los que se protegen la información deben promover reglas que se rijan en el mínimo de riesgos a la base de los datos. Estas normas deben incluir una serie de características como horarios de funciones, restricciones, autorizaciones, denegaciones, perfiles de administradores, técnicas de emergencia, protocolos y todo lo requerido que permita un buen nivel de seguridad de la información. Llevando al máximo a la forma en el desempeño de los, en general y como principal colaborador el uso de programas realizados por programadores. La seguridad de la información nace principalmente para proteger los activos informáticos, principalmente los siguientes:

- **La infraestructura computacional:** se compone principalmente de almacenamiento y administración de los datos, al igual de la forma, el funcionamiento mismo de toda la organización. La función de la seguridad informática en esta área es tener presente un excelente funcionamiento de los equipos previniendo un posible caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier factor que atente contra la infraestructura computacional.
- **Los usuarios:** personas que hacen uso de la estructura tecnológica, zona de comunicaciones y que administran la información. El sistema general debe

¹⁰ SEGURIDAD INFORMATICA. {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en: <https://es.calameo.com/books/00540807863f89223eff9>

estar protegido y los usuarios capacitados para su labor correspondiente de igual forma su labor será certera y no se generarán consecuencias.

- **La información:** esta es el principal activo. Se maneja y está en la infraestructura computacional y es utilizada por los usuarios.¹⁰

7.2.2. Vulnerabilidades

Las vulnerabilidades de un sistema son fallas o posibles riesgos existentes ante un eventual ataque, por tal motivo es de vital importancia tener presente estos aspectos, no existe momento, excepto en donde cualquier individuo haría parte de ejecutar sus aplicaciones dañinas. En base a esta información se citarán tres tipos de vulnerabilidades o afectaciones principalmente que alteran el sistema.

- Vulnerabilidades conocidas sobre apps o métodos instalados. Estas son las que conoce la organización, la cuales amplían las afectaciones de los programas para las cuales ya existe una solución, generalmente se publica en forma de mascara. Existen direcciones de E-mails relacionadas con las noticias de seguridad las cuales hacen el papel de informantes y de detectores de esas vulnerabilidades y propaganda en forma de mascara se puede suscribir.
- Vulnerabilidades conocidas sobre aplicaciones no instaladas. Las organizaciones y los desarrolladores las identifican, al momento de tomar medida no saben cómo actuar porque simplemente no tienen instalada la aplicación correspondiente.

- Según la página Vulnerabilidades ¹¹, Las Vulnerabilidades que no se conocen. No se han sido identificadas por la organización que desarrolla la aplicación, si alguien la detectara podría ser utilizada contra cualquier equipo que tenga instalada la aplicación. Alcanzar que los sistemas y redes trabajen 1005 con seguridad en la información es fundamental para cualquier organización. Esto promueve que las empresas como Microsoft instalen departamentos dedicados únicamente a la seguridad, como es Microsoft Security Response Center (MSRC). El objetivo principal, entre otras, es estar en continuo control de los resultados que los clientes proporcionan sobre posibles amenazas en sus productos, y hacer divulgaciones, revisiones y boletines sobre seguridad que respondan a estos informes. La tabla 1 menciona las vulnerabilidades en función de gravedad, lo que concientiza sobre función de su gravedad, proporcionando una idea de los efectos que pueden tener en los sistemas. ¹¹

¹¹ VULNERABILIDADES. {En línea}. {Consultado el 22 de Febrero de 2018} Disponible en: <http://fpg.hol.es/Seguridad-Informatica-I/vulnerabilidades.html>

Tabla 1 Clasificación de las vulnerabilidades

CLASIFICACION	DEFINICION
Crítica	Este tipo de vulnerabilidad permite la propagación de amenazas sin que sea necesaria la participación del usuario.
Importante	Este tipo de vulnerabilidad es capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios, como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga.
Moderada	Este es uno de los tipos de vulnerabilidades más sencillas de combatir, ya que el riesgo que presenta se puede disminuir con medidas tales como configuraciones predeterminadas, auditorías y demás. Aparte, las vulnerabilidades moderadas no son aprovechables en todo su potencial ya que no afecta a una gran masa de usuarios.
Baja	Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante y su impacto es mínimo. Ya que no afecta a una gran masa de usuarios.

Fuente. <https://tecnologia-informatica.com/vulnerabilidades-informaticas/>

7.2.3. Amenazas

Partiendo del artículo Seguridad Informática¹² Son todas las acciones que tienen la capacidad de hacer daño, atentar contra la seguridad de la información. Las amenazas nacen desde la existencia de vulnerabilidades, es decir de donde una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser potencialmente activa, independiente de que se comprometa o no la seguridad de un sistema de información. Relativos aspectos, como el aumento y la mejora de las técnicas de ingeniería social, la no capacitación y concientización a los usuarios en

el buen uso de la tecnología genera que se incremente la rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

Tipos de amenazas

Según el departamento de Seguridad Informatica ¹², Las amenazas pueden clasificarse en dos tipos:

- Intencionales, en caso de que se lancen o pretenda (por ejemplo el robo de información aplicando la técnica de trashing, la expansión de código malicioso y las técnicas de ingeniería social).
- No intencionales, en donde se producen ejercicios o se dejan de hacer tareas que si bien no buscan explotar una vulnerabilidad, en cambio sí ponen en riesgo los activos de los datos y pueden producir daño (ejemplo amenazas que tiene que ver con fenómenos naturales).

7.3. CÓMO ACTUAR

Cuando existen amenazas o vulnerabilidades, estas solo pueden ser señales de alarma para prevenir daño potencial para cualquiera de los activos informáticos, o dispositivos que contengan información, no es más que una alerta que indica de que el daño al que se está exponiendo o se produjo. Es la razón por la cual se debe

¹² DEPARTAMENTOS DE SEGURIDAD INFORMATICA. {En línea}. {Consultado el 01 de Marzo de 2018} Disponible en: <http://www.seguridadinformatica.unlu.edu.ar/?q=node/12>

estar a la vanguardia con este tipo de incidentes en contra del buen uso de la información, seguido hacer los respectivos reportes de incidentes.

7.3.1. Delitos

De acuerdo con la página Delito Informático¹⁴, Un "delito informático" o "ciberdelito" es toda acción jurídica que lleva a una persona a ser culpable cuando ha incurrido en daños a medios tecnológicos o se ha apropiado de la información de manera abusiva. Se pueden asociar con acciones criminales por vías informáticas ya que según la teoría del delito este no se considera como un crimen, el objetivo principal es prevenir las faltas a los medios informáticos y la realización de actividades que limiten las acciones que vallan en contra del buen uso de la información.

Se denomina delitos informáticos a las actividades ilícitas que:

- Se hacen en el acto mediante el uso de un pc, Tablet, celular, sistemas informáticos u otros dispositivos que permiten comunicación en la red (el principal medio es la informática para realizar los cometidos).

Su único objetivo es afectar la información, presentar perdidas, y una de las principales características de esta es la destrucción e impedir el uso de sistemas informáticos (delitos informáticos). No todos los usuarios hacen uso de su PC para

trabajar o laborar, pero las conductas atípicas, antijurídicas y con declaración de culpabilidad utilizan esto como medio de delito.

Recientemente el Dr. Moisés Barrio Andrés, habla de los ciberdelitos, esta definición afirma aspectos negativos que se derivan de todas las labores que se realizan en Internet, dando como acciones indebidas que se denominan delito, y es así como de cada acción se derivan más y consigo sus propios inconvenientes, ejemplo No se identifica el lugar del ilícito, importante para determinar la jurisdicción y competencia penal para su enjuiciamiento y aplicación de la correspondiente ley penal, los inconvenientes de localización y obtención de las pruebas de tales hechos delictivos, el hecho de no tener regulado y constatar inicialmente las direcciones o los medios en donde nace u ocurren las faltas, la insuficiencia en este tipo de regulaciones legales de los ilícitos.

Existe una red de diligencias procesales las cuales realizan las investigaciones aplicando su conocimiento normativo, teniendo medios investigativos, esto conlleva a la aplicación de técnicas que impliquen seguridad en los sistemas de información.¹³

¹³ DELITO INFORMATICO {En línea}. {Consultado el 01 de Marzo de 2018} Disponible en: https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

Se cita explícitamente de la página delito informático¹³, A tal fin obedece la recientemente promulgada Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, también conocida como Directiva NIS. Esta Directiva impone, por ello, a las entidades gestoras de servicios esenciales, así como a los prestadores de ciertos servicios digitales considerados clave en el funcionamiento de Internet, la obligación de establecer sistemas de gestión de la seguridad de la información en sus organizaciones y de notificar a las autoridades los incidentes que tengan especial gravedad. Además, obliga a los Estados miembros a supervisar el cumplimiento de estas obligaciones y a velar por que existan equipos de respuesta a incidentes de seguridad con capacidad para proteger a las empresas de la propagación de estos incidentes. Así mismo, impulsa la cooperación entre autoridades nacionales y el intercambio de información como medio para elevar el nivel de seguridad en la Unión Europea frente a amenazas de carácter transfronterizo.

4.2.1. Riesgos

Basado en departamento de seguridad informática¹⁴ El análisis de riesgos informáticos es una tarea la cual identifica los activos informáticos, sus vulnerabilidades y amenazas para los cuales se exponen del mismo modo la probabilidades que existen en la ocurrencia y el impacto de las mismas, para lograr

determinar cuáles serían los controles adecuados para lograr reducir las afectaciones y evitar la ocurrencia del riesgo.

Se debe tener en cuenta, cuando un riesgo no se le da la debida importancia puede causar graves daños, pérdidas financieras, administrativas, el objetivo es poder concluir a que impacto del riesgo se encuentra expuesto el activo usando técnicas y controles.

Generalmente toda la recopilación de las afectaciones y las medias que se tomen, para cada causa, llegaran a fomentar una arquitectura fortalecida para combatir las inseguridades bajo las participaciones de confidencia, integridad y disponibilidad de las partes de los objetos de riesgo.¹⁴

Herramientas de Apoyo

Actualmente hay un sin número materiales que se pueden utilizar y sirven de base a la hora de que exista algún tipo de riesgo, proceso que se debe de analizar de principio a fin. Cada uno de los aspectos a combatir se debe de documentar, recabar y posteriormente analizar. De esta forma las herramientas serán más efectivas a la hora de combatir alguna vulnerabilidad, la importancia siempre partirá de su

¹⁴ DEPARTAMENTOS DE SEGURIDAD INFORMATICA. {En línea}. {Consultado el 01 de Marzo de 2018} Disponible en: <http://www.seguridadinformatica.unlu.edu.ar/?q=node/1210> DELITO INFORMATICO {En línea}. {Consultado el 01 de Marzo de 2018} Disponible en: https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

interpretación y selección se reitera de esta forma se ahorraría una gran cantidad de costo en productos y ahorro de tiempo.

7.4. MARCO LEGAL

Citando explícitamente la norma LEY 1273 DE 2009 ¹⁵, en la actualidad los ataques se hacen populares. En Colombia se ve afectada la seguridad de la información en grandes organizaciones de aquí parte la necesidad de comprender y cumplir la legislación que corresponde a los derechos de autor: Decisión 351 de la CAN: Se presenta para reconocer los derechos del autor y dar protección sin distinguir el tipo de arte.

- Ley 23 de 1982: Ley sobre los derechos de autor, presenta toda la regulación correspondiente a los derechos de autor en Colombia.
- Ley 44 de 1993: Esta modifica la Ley 23 de 1982 y la ley 29 de 1944, se adicionan nuevas disposiciones como el soporte lógico (Software).
- Ley 545 de 1999: Por la cual se aprueba "Tratado de la OMPI -Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT)" que contempla los derechos de propiedad intelectual de los artistas cantantes músicos, los productores etc., que tengan responsabilidad de los sonidos interpretación o ejecución.
- Ley 603 de 2000: Por la cual se modifica el artículo 47 de la Ley 222 de 1995.

Contamos además con la legislación con respecto comercio electrónico y firmas digitales:

- Ley 527 de 1999: esta ley reglamenta principal el acceso y uso de mensajes de datos y comercio electrónico y de las firmas digitales, esta ley se divide¹⁷
- Citando explícitamente la norma LEY 1273 DE 2009 ¹⁵, en dos partes, primero permite el uso de información o datos para el comercio electrónico, firmas digitales, mensajes de datos por medio escrito y digital, también permite la certificación de las personas naturales y jurídicas para realizar transacciones electrónicas, pero además da reconocimiento legal a los documentos electrónicos como si fueran físicos y pueden ser parte de un proceso legal.
- Decreto 1747 de 2000: por la cual se reglamenta la Ley 527 de 1999.
Resolución 26930 de 2000: “Por la cual se fijan estándares para la autorización y funcionamiento de las entidades de certificación y sus autores”

También tenemos leyes de protección de datos personales:

- Ley 1581 de 2012: Esta ley dicta disposición sobre la protección de datos personales. Se trata básicamente de reconocer el derecho que tiene toda persona de conocer, actualizar y rectificar los datos que se hayan recogido

¹⁵ LEY 1273 DE 2009. {En línea}. {Citado el 26 de Septiembre de 2017} Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

sobre cada una en bases de datos, así como reconocer el derecho constitucional referido en el artículo 15 de la constitución política de Colombia que se refiere principal al derecho a la intimidad y el artículo 20 que se refiere al derecho de informar y recibir información veraz.

- Ley 1266 de 2008: en la cual se dictan disposiciones del hábeas data y se regula la información el manejo de la información que está contenida en las bases de datos especialmente financieras y crediticias.

CAPITULO. I

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva.¹⁶

Citando explícitamente la norma LEY 1273 DE 2009 CAPITULO. II

- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17

¹⁶ LEY 1273 DE 2009. {En línea}. {Citado el 26 de Septiembre de 2017} Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

- Artículo 58. Circunstancias de mayor punibilidad.
- Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6.¹⁶

8. ESQUEMA TEMATICO

8.1. CAPITULO I SMART TV

En la actualidad el auge de la tecnología e internet tienen sumergidos a la gran mayoría de gente, esto trae consigo que la información que se maneja a diario: fotos, video, números, texto se encuentra vulnerable a un sin número de aspectos como perdida, robo, plagio, porque el hecho no es solo navegar en esta red sin usar normas, reglas, parámetros si no se tienen en cuenta esto se estaría dando un mal uso a la información, entre las consecuencias más graves tendríamos el secuestro de la misma y si en tal caso no se cuenta con una copia de seguridad, se vería comprometidas las actividades que se realizan, dinero tiempo en fin.

En la mayoría de los casos los usuarios que utilizan su conocimiento tecnológico para realizar delitos informáticos lo hacen con fines económicos, dañinos o simplemente por gusto, aspectos principales que los caracteriza. Continuando la información es un todo y es la herramienta fundamental para cualquier operación indiferente de la organización, producto o servicio que se ofrezca, actualmente existen varias herramientas, aplicaciones y día a día se crea conciencia en los usuarios para que se eduquen en el tema de seguridad de la información, sepan que es un grave problema no asegurar o tener las mínimas precauciones de protección; como es sabido la mayoría de los procesos se realizan mediante un computador, celular, Tablet y últimamente las características de estos dispositivos se implementan en los

televisores inteligentes Smart TV, igualmente y con las mismas posibilidades de generar un sin número de vulnerabilidades a la información, la cuales se presenta en cualquiera clase de estos dispositivos independiente de la marca o tamaño físico, el objetivo siempre será la información contenida la cual es el punto débil de los usuarios.

8.1.1. Historia

Según la página Historia de la televisión ¹⁷, el fin de la TV a través de los tiempos fue pretender reproducir retransmisiones radiofónicas, tanto a noticieros como a relatos o radionovelas.

Del mismo modo dar a conocer la conexión visual del mundo exterior. En términos generales en planeta su expansión se produjo antes, su primera reproducción se disfrutó en 1956. Las primeras emisiones fueron en blanco y negro. Los espectadores a un tipo de televisión tipo cine por lo que fue aceptada sin inconvenientes, no tuvieron mayor perspectiva y no influyo de forma negativa en su éxito.

A través de los años se divisaban solo dos canales, su objetivo era reunir el grupo familiar en donde se disfrutaba un tipo de señal satelital. Hablando de economía fue una forma de democratizar la cultura. Pasa un tiempo llegaron los reproductores de

¹⁷ HISTORIA DE LA TELEVISION {En línea}. {Citado el 26 de Septiembre de 2017} Disponible en: https://es.wikipedia.org/wiki/Historia_de_la_televisi%C3%B3n

video, partiendo de la página Historia de la televisión¹⁸ los DVD se suma también, los *Home Cinema*, y sí, ya se pudo decir que la experiencia del cine había llegado a casa.

La forma de ver televisión fue cambiando en cuanto a forma y señal, estirando, aplanando, y ganando una calidad de imagen extraordinaria, este prototipo se mantuvo hasta que llegó la Internet, teniendo en cuenta que las conexiones de banda ancha permitían servicios como YouTube (videos hechos en casa), VEVO (se cambió por MTV), la dependencia de horarios para ver cierto contenido estaba pasando de moda. Teniendo en cuenta esto la nueva tecnología Smart TV e Internet evolucionaban a un ritmo exponencial, estos con la característica principal de inteligencia integrada widgets, empezaron a coger fuerza y a adquirir funciones muy convenientes como ofrecer información meteorológica y acceso rápido a la búsqueda de Google o YouTube. Pasado el tiempo, la televisión se convirtió en un accesorio tradicional consiguiendo su propio espacio, de esta forma se sustituyó completamente a la televisión de siempre con la llegada de servicios de entretenimiento. Al ver la importancia futura, los canales clásicos se pusieron a la tarea de lanzar sus propias aplicaciones de contenido, lo que le siguió fue la explosión en otros mercados de servicios como Netflix.

El solo hecho de llegar a casa y encontrar una serie favorita en Netflix o en Wuaki no tiene precio como se pensaría coloquialmente, pero con un Smart TV es posible ver la pantalla de nuestro ordenador o móvil en el televisor, ideal para enseñar a

familiares las fotos de un viaje, o ver mejor las de nuestros contactos en redes sociales.¹⁸

Actualmente se puede usar la pantalla del TV como monitor, permitiendo así divisar juegos en línea u contenido de la web como Gamefly, el solo hecho de que el usuario disfrute en línea lo que anteriormente era demorado y engorroso actualmente todo es menos complicado, las herramientas de estos dispositivos son casi que intuitivas y aunque no se crea en un futuro será suprimido el teclado, mouse, controles y todo se manejara por comandos de voz y señas.

Las afectaciones familiares sobresaltan el sentido de participación y comunicación ya que, pese a haber sufrido cambios con el avance de los tiempos, vuelve a situar su atención en la TV, contenidos, juegos y aplicaciones de los cuales hacen uso, un Smart TV llega a ser algo incluso social, las aplicaciones se pueden compartir, guardar en la biblioteca música, compartir vídeo y fotos con nuestros amigos sacando provecho al máximo con las nuevas conexiones de fibra. Permitiendo que las funcionalidades adaptadas al siglo XXI tenga una novedad al 100%, aunque esta contenga este sinnúmero de aplicaciones para usar no hay que dejar a un lado que la televisión seguirá siendo durante muchos años más, la misma de siempre, el

¹⁸ La historia de los televisores, descubre su evolución {En línea}. {Citado el 26 de Septiembre de 2017} Disponible en: <https://computerhoy.com/noticias/imagen-sonido/historia-televisores-descubre-su-evolucion-7161>

cambio está en su forma física y características adicionales nombradas anteriormente.¹⁹

Vemos que, si se quiere disfrutar de contenidos en varios lugares del hogar, era necesario, o bien adquirir varios televisores, o bien transportarlos. En cierto modo es algo incómodo por su tamaño y cuidado. La personalización de las interfaces son una alternativa al launcher tradicional de Touch Wiz, presentando las aplicaciones multimedia en mosaicos, que hace que nuestra mano sea el mando a distancia.

Reiterando sus características físicas tamaño de pantalla, se puede complementar al del monitor de nuestro ordenador, tanto para ayudar en la visualización de documentos como para edición y producción de datos, haciendo conexiones de bluetooth externo o incluso un ratón. A medida que los Smart TV evolucionan, se muestra más como una solución productiva, y trabajo con el modo OTG permite conectar pendrives y discos duros externos puede ser el primer paso hacia la convergencia.

8.1.2. Evolución

El éxito de los Smart Televisor ha logrado un impacto favorable en el mercado para todo tipo de usuarios, al mismo tiempo genera que según la evolución del TV no se

¹⁹ Historia de la televisión: Inventor Origen y Evolución {En línea}. {Citado el 26 de Septiembre de 2017} Disponible en: <https://historiaybiografias.com/television/>

pueden evitar. El camino que ha tenido su acelerada evolución tal vez no fue el esperado ²⁰

Figura 1 Evolución de la Televisión



Fuente. <https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

En Medio siglo los televisores han venido considerando como algo imprescindible en el hogar a lo largo del planeta, como es sabido los primeros aparatos se mostraron en líneas blanco y negro, a partir del año 1972 se incorporó la primera TV a color en donde su proyección era muy atrayente por su gama de colores.

²⁰ EVOLUCION DEL TELEVISOR {En línea}. {Citado el 16 de Septiembre de 2017} Disponible en: <https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

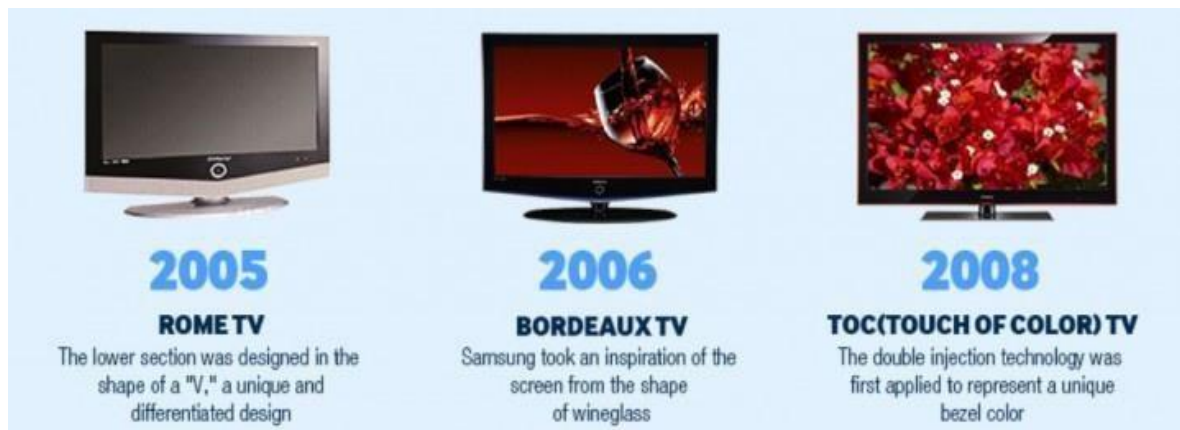
Figura 2 Evolución de la Televisión 2



Fuente. <https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

Según la evolución del Televisor En los años 90 el **control remoto** y diseño más sofisticado en su pantalla popularizo aún más este dispositivo, por su control sin tener que levantarse de la silla, con un formato y una pantalla más amplia aumentaba el disfrute de los espectadores.

Figura 3 Evolución de la Televisión 3



Fuente. <https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

En el nuevo milenio sufrió un cambio extremo, los diseños planos y extendidos, simulando pantallas gigantes, a su vez la llegada de los dispositivos HD Ready,

permitían que su ubicación fuera cómoda y de alguna forma llamativa para el usuario.²¹

Figura 4 Evolución de la Televisión 4



Fuente.<https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

²¹ EVOLUCION DEL TELEVISOR {En línea}. {Citado el 16 de Septiembre de 2017} Disponible en: <https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

Según la evolución del Televisor ²² Aparecen los televisores LED (Pantallas con gas en el interior) retroiluminación LED, ligada al comercio de dispositivos Full HD mejor calidad en la imagen marcaron la gran evolución.²⁵

Figura 5 Evolución de la Televisión 5



Fuente. <https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

Con la llegada de los televisores inteligentes, vienen cambios radicales en su funcionamiento, como es sabida sus numerosas aplicaciones permiten la conexión a internet y acceder a servicios de la red, y con este las numerosas vulnerabilidades que se crean a la hora de manipular información.

²² EVOLUCION DEL TELEVISOR {En línea}. {Citado el 16 de Septiembre de 2017} Disponible en: <https://www.adslzone.net/2015/02/07/45-anos-evolucion-televisor/>

8.1.3. Futuro

El solo hecho de que un dispositivo pueda tener acceso a la red tiende a sufrir vulnerabilidades y de ser infectado por virus, es un grave problema, actualmente los atacantes se están aprovechando para infectar con virus a los Smart TV, el 90% de los televisores conectados son vulnerables. Teniendo en cuenta la página que puede pasar con los televisores del futuro ²³ Los creadores de malware mejoran continuamente sus tácticas y no hay ninguna duda de que van en evolución. Los elementos con que cuenta estos dispositivos son gran atractivo para ciber ataques, micrófonos o incluso cámaras, son inspiraciones para robar datos confidenciales, hacer espionajes, y dar permisos peligrosos podrían ser en este caso instalación de App desconocidas.

Uno de los Malwares más populares identificados scripts para minar criptomonedas, usualmente estos suelen ralentizar el dispositivo, generalmente los usuarios no se dan cuenta ni lo detectan.

Dentro de las aplicaciones instaladas hay una en particular que busca suplantar portales de intercambio en este caso Poloniex, donde se falsifican las opiniones de su funcionamiento. Generalidades de infecciones:

²³ QUE PUEDE PASAR CON LOS TELEVISORES EN EL FUTURO {En línea}. {Citado el 16 de Septiembre de 2017} Disponible en: <http://www.eltiempo.com/tecnosfera/dispositivos/el-futuro-de-los-televisores-153420>

Medio de pago. La tecnología avanza a pasos agigantados, una característica importante que se realiza con el chip NFC (Near Field Communication) es la comunicación inalámbrica que según la página que puede pasar con los televisores del futuro admite la transmisión de datos entre dispositivos a unos 5-10 centímetros, y que se utiliza para realizar pagos, transferir información, etc. Una de las ventajas de este tipo de comunicación nace en la velocidad de emparejamiento, el consumo, y su compatibilidad con RFID²⁵ (Radio Frecuencia Identificación).

Aplicaciones Bancarias. Los bancos crean sus propias aplicaciones para este tipo de dispositivos, a su vez crea la posibilidad de que el malware utilice mejores técnicas para interceptar transacciones que recepcionarán información sensible es muy alta.

Seguimiento de individuos. Las señales de los dispositivos móviles las cuales incorporan GPS, se hace necesario y vital desarrollar apps que a la hora de consultarse, entreguen una señal de ubicación como coordenada en el GPS, las cuales tengan la capacidad de hacer detecciones de posibles atacante en los servidores, si en algún caso se presenta robo seria de vital importancia para la localización del dispositivo.

Vulnerabilidades por redes Wi-Fi. Los Smart TV se componen de conexiones integradas a las redes Wi-Fi, se podría pensar en la idea de que puedan existir

gusanos que investiguen sigilosamente los sistemas que se componen red Wi-Fi, e infiltren códigos maliciosos a estos sistemas explotando sus vulnerabilidades.

Ataques de ingeniería social avanzada. No se es exento de existencia de malware el cual puede tener la capacidad de cambiar la agenda personal de un usuario, lo cual puede ser muy útil para hacer uso de su identidad, asociando un número a otra persona, utilizando ingeniería social orientada.

8.2. CAPITULO I CARACTERISTICAS Y PARAMETROS DE SEGURIDAD EN LA TRASMISION DE DATOS PARA LOS SMART TV

Teniendo en cuenta las diferentes fuentes consultadas, se resaltan los siguientes ítems.

- Basados en 6 características de los Smart TV se resalta lo siguiente, permite a los usuarios compartir contenidos multimedia a través, DNLA (Siglas en ingles alianza para el estilo de vida digital en red) y acceder a contenidos basados en internet, tales como video, fotos, audio y canales de TV por Internet ²⁴. Dentro de las aplicaciones móviles permite recepcionar contenido desde los Smartphone, sincronizar canales, dar seguimiento a redes sociales.

²⁴ SEIS CARACTERISTICAS DE LOS SMART TV {En línea}. {Citado el 16 de Marzo de 2018} Disponible en: <https://www.nacion.com/viva/moda/seis-caracteristicas-de-los-smart-tv/CBY2X3A4BBCUDKO3MNQNPUEZY/story/>

- Ciertos modelos de Smart TV, mediante la utilización de gestos, inclusive la voz, controlan el dispositivo.
- Permite la descarga de videojuegos aparte de su utilización en línea.
- Tienen acceso a bluetooth, permitiendo así compartir contenido de música.
- Existen varias marcas que ofrecen tecnología 4k, resolución en la imagen más conocida como Full HD.
- Menú intuitivo, wifi integrado, plataforma de navegación.

Figura 6 Smart TV



Fuente https://i.blogs.es/f98768/que-20es-20un-20smart-20tv/1366_2000.jpg

8.2.1. Proveedores

Teniendo en cuenta el artículo siete aplicaciones para tu televisor ²⁵ se cita explícitamente el siguiente.

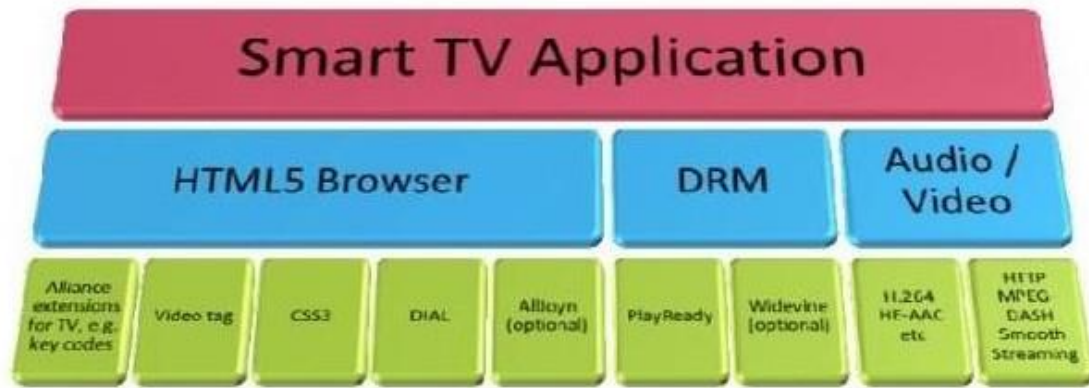
- LG Smart TV (de LG).
- Samsung Smart TV (de Samsung).
- Sony Internet TV (de Sony).
- Panasonic Smart Viera (de Panasonic).
- Philips Net (de Philips) basado en los estándares Open IPTV Forum.
- Web: TV (de Blusens).
- Smart (de Hisense).
- E M P Series (de Vizio).
- Toshiba Smart (de Toshiba)

8.2.2. Arquitectura

Smart TV (Figura 2) muestra que la arquitectura maneja los teléfonos es similar a la de los Smart TV, se pueden ver tres capas en términos. Engine se compone de un conjunto de librerías esta maneja todo lo relacionado con estilos, gráficos, redes, broadcasting base de datos, etc., esto significa los drivers y componentes de bajo nivel ligados al Sistema Operativo. ³⁰

²⁵ SIETE APLICACIONES PARA TU TELEVISOR {En línea}. {Citado el 16 de Marzo de 2018} Disponible en: <http://www.samsung.com/es/a-fondo/contenidos-y-servicios/7-aplicaciones-para-tu-televisor-samsung-smart-tv/>

Figura 7 Aplicaciones de los Smart TV



Fuente. <http://www.samsung.com/es/a-fondo/contenidos-y-servicios/7-aplicaciones-para-tu-televisor-samsung-smart-tv/>

Partiendo de la idea de la página siete aplicaciones para su televisor, cada una de las capas intermedia administra las partes fundamentales que permite que la plataforma este en mejora continua en cuanto a aplicaciones tipo browser para diferenciar el contenido web, multimedia, y control DRM4 (Digital Right Management). La tercera capa o capa de aplicación es la conformada de las aplicaciones finales, widgets, contenidos, servicios, y juegos que es justamente lo que se observa en la pantalla del Smart TV.

6.1.2. SISTEMA OPERATIVOS, PROTOCOLOS Y POLITICAS.

Actualmente existen diferentes plataformas que a través de la historia se han mantenido presente en el mundo tecnológico. Precisamente mencionando a los computadores con Linux, Mac y Windows, los teléfonos móviles con Android,

Windows pone, los cuales parten de mejorar aplicaciones populares para cada plataforma, si bien es cierto los SO disponibles en teléfonos y tablas también fusionan en los Smart TV, la mayoría de su Sistema está basado en código abierto.

Tabla 2 Sistemas Operativos

Smart TV	Sistema Operativo
Google TV	Android
Samsung Smart TV	Linux
LG	WebOs (Linux)
Apple TV	IOS
Toshiba	Linux
TCL UltraSurface	Windows 8
Sony	Linux
Panasonic	Linux

Fuente. Smart TV y sus Sistemas Operativos

Actualmente el más empleado es Android, como se mostrará en la siguiente tabla la mayoría de estos dispositivos utilizan Linux como Sistema operativo base, seguido por Android. En la actualidad el software libre sigue siendo el más usado para el desarrollo de los dispositivos inteligentes.

Android TV: con la evolución de la tecnología y desde que se presentaron los primeros celulares con tecnología inteligente Android que básicamente es una distribución de Linux donde su evolución impresiono con continuos cambios a lo

largo de periodos muy cortos, actualmente este sistema operativo es el más usado dentro de la línea de teléfonos inteligentes y g Smart TV. Actualmente esta plataforma permite a operadores y desarrolladores mejorar su funcionalidad ya que es código abierto. Ofrece la posibilidad de contar con aplicaciones comunes entre los celulares y tablet's, por tal motivo es uno de los más usados porque permite ser compatible con múltiple tecnología celular, dispositivos de audio y video.

Este sistema operativo ofrece a los usuarios ejecutar aplicaciones como YouTube, Hulu Plus NBA Game Time, a la vez permite a los usuarios ejecutar los contenidos por medio de comandos de voz.

A su vez permite ejecución en google donde básicamente se pueden hacer las mismas funciones como en el pc o en el dispositivo móvil, una de las principales características es que soporta a la vez 4 dispositivos.

Tizen Os: Esta plataforma en basada en Linux, pero su modelo no es de código abierto contiene licencias para su uso, para el desarrollo de las plataformas de Samsung este pública una SDK de código no abierto, aunque muchos de sus características pertenecen a código abierto. Los desarrolladores de Samsung incluyeron características como animación en el inicio, calendario, gestor de actividades, reproductores bajo una licencia de Flora Lucense la cual es difícil que sea compatible con futuros modificaciones o ediciones de estas aplicaciones.

Generalmente este sistema operativo lo utilizan los Smart TV de la marca Samsung como se menciona anteriormente, las aplicaciones más características son Smart View y Smart Hub el cual es un menú de acceso rápido a los contenidos del dispositivo, al igual que el sistema operativo androide sincroniza dispositivos móviles y reproduce contenido en alta definición es compatible con Adroid 4.1 y superior o IOS 7.0 y superior.²⁶

Web OS: este sistema operativo tiene sinónimos como LG WebOs, open WebOs y HP WebOs, este sistema operativo permite ejecutar múltiples tareas en los dispositivos inteligentes es una base de Linux, inicialmente fue creado para estos medios, aunque posterior lo adquirió HP, su código es libre y utiliza una interfaz gráfica moderna, permite hacer actualizaciones mediante wifi a sus dispositivos. Este sistema operativo lo utiliza la marca LG, esta plataforma es más grafica intuitiva para los usuarios es un hijo de Linux, ofrece hacer uso de canales de forma ordenada y optimizar las aplicaciones más relevantes para los usuarios su control remoto es mágico y se asemeja a un curso en la pantalla, permite descarga de contenidos y memoria para salvarlos es compatible con casi todas las marcas de los dispositivos móviles que sirven para sincronización de contenidos.

²⁶ REVISTA GAGET {En línea}. {Citado el 16 de Marzo de 2018} Disponible en: <http://www.revista-gadget.es/reportaje/sistemas-operativos-televisor/>

Los televisores inteligentes o también llamados Smart TV, están diseñados bajo plataformas que manejan código abierto como se presentan anteriormente que se desarrolla o se distribuye sin ningún tipo de restricción o costo, este tipo de código generalmente se denomina Software libre cuyo código fuente se puede modificar con libertad y sin tipos de licencias, su **objetivo principal** está dirigido a compartir código por ende quien modifique un código abierto debe de presentar un calidad superior al software original debe de tener calidad, el software libre resalta acceso a código, software gratis o libre, no hay dependencias de fabricantes o monopolios, modelos avanzados no están ocultos solo modificaciones y superioridad de software. A continuación, se muestran una serie de programas de código abierto para tener referencia. Para poder desarrollar en código abierto se debe de tener en cuenta lo siguiente. Su redistribución será de venta libre o regalada.

- El código se puede conseguir de forma libre.
- Todas las modificaciones a las redistribuciones se deben permitir.
- No debe haber discriminaciones de licencias.
- Ningún usuario puede se puede excluir independiente del área o tema que maneje.
- La licencia no debe se explicita de un solo producto.

Entre las plataformas de software libre que se encuentran actualmente y que son utilizadas por un sin número de usuarios según facilidad de conocer código se distinguen las siguientes.²⁷

Partiendo de la página que sistema operativo para Smart te conviene más²⁸

- Los sistemas operativos más populares son, Red Hat (Centos), Ubuntu y Debian, basados en Linux. Android, de Google, para relojes, Smart TV, teléfonos inteligentes y tabletas.
- Entre los programas de código abierto en diferentes teniendo en cuenta las diferentes sitios, se destacan las suites ofimáticas Libre Office y Open Office, navegador Firefox, el cliente de correo electrónico Thunderbird, reproductor multimedia VLC, editores de imágenes GIMP o Inkscape, editor de video Kdenlive, editor de audio Audacity, videojuegos Fretsonfire, 0 A.D.
- Antivirus como el Clam Win.
- Programas, Apache Software Foundation y Github
- El lenguaje de programación de Apple Swift 2.
- Plataformas de enseñanza como Moodle (un ejemplo es Moodle)

²⁷ REVISTA GAGET {En línea}. {Citado el 16 de Marzo de 2018} Disponible en: <http://www.revista-gadget.es/reportaje/sistemas-operativos-televisor/>

²⁸ QUE SISTEMA OPERATIVO PARA SMART TV TE CONVIENE MÁS {En línea}. {Citado el 16 de Marzo de 2018} Disponible en: http://www.parentesis.com/tutoriales/Sistemas_operativos_mas_populares_para_Smart_TV

Para el desarrollo de los sistemas base de los **Smart TV** el SO operativo utilizado de forma libre es el **Android** ya que este mediante la conexión del dispositivo a través de la red de internet se actualiza solo o automáticamente.

Android es un SO bajo el Núcleo Linux software no privativo pionero de software libre y código abierto, su diseño está enfocado principalmente para dispositivos como:

- Automóviles Dispositivos móviles con pantalla táctil.
- Tabletas
- Teléfonos inteligentes
- Televisores Smart TV
- Relojes Inteligentes
- Dispositivos móviles con pantalla táctil

El avance y la acogida por los usuarios presentan un éxito de casi un 100% a la facilidad de manipulación y grandes beneficios que ofrece.

Protocolos utilizados por esta tecnología

UPnP (Universal Plug and Play) es un protocolo de comunicación su función es permitir que los periféricos en red como pc, impresoras, Smart TV, dispositivos móviles, blue ray, exista comunicación permitiendo compartir datos información y

exista entretenimiento. Al tener implementado este protocolo como el DHCP, permite que exista fuga de información o que estos dispositivos sean expuestos a vulnerabilidades cibernéticas, los dispositivos pueden enviar paquetes a la red privada seguido los dispositivos UPnP responden haciendo saber que el servicio está activo, el dispositivo sigue enviando paquetes para preguntar a qué servicios puede acceder. Uno de los inconvenientes que se pueden presentar es que los dispositivos respondan a los mensajes, si es el caso un malware hace respuesta infectando el dispositivo y permite abrir un agujero en el firewall para ya no depender de estos mensajes si no de lo contrario ingresar directamente. Caso puntual

Citando Universal Plug and play un ejemplo, **BitTorrent** es un cliente UPnP, cuando se ejecuta en una red no publica, identifica al Router mediante UPnP y le verifica su IP externa. La IP pública no es conocida dentro de la red privada, bittorrent requiere distinguirla para permitir comunicación con otros usuarios bittorrent y establece conexiones. Seguido BiTorrent hace uso de un puerto abierto, de esta forma se modifica la configuración del Router dando paso a bitTorrent recibir tráfico entrante no solicitado. Durante el tiempo transcurrido que UPnP lleva funcionando, nadie sugiere que esto debiera estar funcionando en el lado público del router. El diseño de UPnP solo en el lado privado de la red, es decir, en la red de casa, del trabajo, etc ²⁹.

²⁹ UNIVERSAL PLUG AND PLAY {En línea}. {Citado el 21 de Abril de 2018} Disponible en: https://es.wikipedia.org/wiki/Universal_Plug_and_Play

Es preocupante saber que la IP queda descubierta a un hacker y de este modo se interrumpe el proceso de comunicación del UPnp hacia el router y en cambio se suplantaría la autenticación del protocolo.

IPTV (Protocolo de Televisión) se hace necesario cuando se requiere para los Smart Tv suscripción de señales de TV, cuando estas conexiones requieren o hacen necesario usar banda ancha sobre el protocolo IP.

Los usuarios confunden la televisión en línea cuando en realidad es televisión sobre IP, generalmente este último hace que la señal o el servicio de televisión se preste de forma eficiente. Este protocolo funciona cuando el cliente se conecte y requiera del servicio cuando no halla conexión lo puede hacer habilitando las opciones requeridas, sus partes son: adquirir la señal de video los proveedores de internet o que distribuyen señales de televisión le dan permiso a estos protocolos para que digitalicen y compriman el video, poder almacenar servidores de video y calidad de video como VHS,DVD,WMV, MPGE-4, videoconferencia, videotelefonía, calidad alta y transmisión de baja, distribuir su contenido permite alta calidad y velocidad en la transferencia decodificando la información para poder visualizarla de forma tradicional.

Adicionalmente las ventajas que ofrece este protocolo no hay etiqueta para manipulación de la información, necesariamente el router no conserva información del proceso. Desventajas debe tener la comunicación activa por cada router que

pasa señalando su espacio, a los paquetes que van en transporte se les asigna una prioridad.

Este protocolo da paso a la televisión IP acceso de reproducción de televisión en línea.

Widi (Intel Wireless Display) Transmite contenido como imagen, sonido inalámbrico desde un dispositivo remoto como teléfono, pc a los Smart TV, de esta forma se omiten todo tipo de cables, estas conexiones son permitidas partiendo de unas características especiales de los dispositivos como el tipo de procesador desarrollados a partir del año 2010.

En su configuración permite reproducir contenidos almacenados en los dispositivos, su principal característica es la forma intuitiva de manejarlo, es casi que automático mediante la ejecución del WIDI los dispositivos lo detectan, inicialmente el usuario introduce su password de 4 dígitos para vincular los dos equipos y poder tener acceso a la televisión estándar. Entre las ventajas esta la eficiencia para transmitir archivos, emisión de video en alta definición, permite una velocidad de entre 10 y 28 gb por segundo compatible con HDCP este permite el streaming desde el Blu-ray o DVD, esta tecnología es segura ya que sus contenidos están protegidos por un sistema anticopia.³⁰

³⁰ WIDI {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <https://es.wikipedia.org/wiki/WiDi>

Miracast permite transmitir datos audio y video mediante conexión a una red WIFI de alta definición a distintos dispositivos, de tal modo todo el contenido interactivo será accesible gracias a este protocolo, al igual que el WIDI hay que tener en cuenta las características de los dispositivos. También es llamado Display Mirroring múltiples industrias incluyen esta tecnología en sus dispositivos ya que permite compartir contenido entre diferentes dispositivos reproducción de archivos y de televisión en tiempo real, la vinculación de estos dispositivos teniendo un ejemplo claro bluetooth el cual busca una integración para poder disfrutar de todas las aplicaciones.³¹

WEP protocolo de comunicación da paso a que dos o más dispositivos permita el traspaso de información tanto de software como hardware. (Identifica el protocolo de acceso a la DNS o IP del servidor) WPA/PSK, WPA2/PSK. Distribución de llaves para usuarios, permite la creación de contraseñas para poder conectarse a puntos de acceso codificados. (Autenticación se base en PSK clave compartida previamente para proteger las comunicaciones inalámbricas. Tipo de Cifrando: WEP, TKIP, AES.). Este hace una denominación de las normas y pautas que se emplean para seguir los procesos de las acciones que se realicen en la red, mediante este protocolo se establecen las comunicaciones de los diferentes

³¹ MIRACAST {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <https://es.wikipedia.org/wiki/Miracast>

componentes del sistema de interconexión en general mediante este protocolo los dispositivos se conectan y pueden hacer recepciones mutuas de datos ³².

8.2.3. Vulnerabilidades en la seguridad de los Smart TV.

Este tipo de tecnología Smart TV permiten vivir una experiencia realmente mejorada, teniendo en cuenta que sus características permiten visualizar una calidad de la imagen superior 3d, sonido y rapidez de conexión ya que permite la conexión a la red y al igual que una Tablet o teléfono se pueden realizar procesos similares como navegación en redes sociales, cuenta de correo electrónico y pagos electrónicos, operaciones frecuentes de los usuarios, estas últimas actividades se realizan sin ningún detenimiento de seguridad, sistema de autenticidad, firewall o antivirus, no incluyen barreras de protección, hay que tener en cuenta que los modelos de seguridad serían una gran herramienta para prevenir vulnerabilidades ³³.

Teniendo en cuenta lo descrito en Vulnerabilidades de seguridad en Smart TV, los planes de seguridad deben estar soportados por políticas y procedimientos que definan porque, para qué y cómo proceder para alcanzarlo, es una regla general evitar problemas, la vulnerabilidad de la seguridad en las redes y sistemas operativos, es un tema que es de intereses y que merece respeto, por tal motivo

³² PROTOCOLO DE INTERNET {En línea}. {Citado el 21 de Abril de 2018} Disponible en https://es.wikipedia.org/wiki/Protocolo_de_internet

³³ VULNERABILIDADES DE SEGURIDAD EN SMART TVS Y LAS CONSECUENCIAS EN SU PRIVACIDAD {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <https://www.xataka.com/televisores/vulnerabilidades-de-seguridad-en-smarttvs-y-las-consecuencias-en-tu-privacidad>

hay que tener en cuenta cual es nuestro fin en proteger, esta información se divide fundamentalmente en las siguientes partes:

- Seguridad Física
- Seguridad de la red
- Seguridad del host
- Seguridad de las aplicaciones
- Seguridad de los datos

Los procesos de seguridad deben abarcar las anteriores ya que todas conforman un sistema completo que forma parte de la organización y por tanto debe estar unificado y girar en torno de todos, ya que de este modo se previenen ataques tanto internos como externos.

La idea principal de la Monografía es condensar características y parámetros de la seguridad en la transmisión de datos para dispositivos Smart TV. El desarrollo de sus objetivos permitirá hacer parte de una educación tecnología o guía para el uso de este dispositivo, protección de los datos del usuario cuando este a través del dispositivo acceda a la red y su navegación no sea víctima de vulnerabilidades actualizaciones en periodos de tiempos determinados y mayor capacidad en cada etapa de desarrollo.

Una característica importante que requiere poner al tanto a los usuarios es que este dispositivo no cuenta con Firewall, antivirus o requisitos de autenticación de usuario como es habitual en un computador personal o teléfono y puede sufrir ataques remotos, es una plataforma que es vulnerable ya que no posee mecanismos de seguridad de la información y se puede presentar robo de datos, espionaje si este cuenta con web cam, este sistema que presenta ataques de tipo DNS para conseguir historial de búsqueda en cache del usuario y la contraseña que se usa para acceso a la red, se puede explotar remotamente otorgando derechos a información contenida en el disco duro o en la USB.³⁴

Los mismos proveedores pueden mediante dispositivos capturar comandos de voz y textos para valorar y mejorar aspectos relacionados con su funcionalidad, pero hay que tener en cuenta que si en las conversaciones se incluye información privada o sensible estos datos puede ser trasferida a empresas o terceros.

Los ataques están diseñados bajo lenguajes como JavaScript o HTML5, los televisores no están optimizados en cuanto a medidas de seguridad.

Es sabido que su conexión a la red de internet es por medio de Ethernet o wifi, esta tecnología utiliza chips para poder hacer reproducción de video, pantallas múltiples y hacer conexiones a la red, aparte que hacen uso de una memoria para el

³⁴ VULNERABILIDADES DE SEGURIDAD EN SMART TVS Y LAS CONSECUENCIAS EN SU PRIVACIDAD {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <https://www.xataka.com/televisores/vulnerabilidades-de-seguridad-en-smarttvs-y-las-consecuencias-en-tu-privacidad>

procesamiento de los procesos como controlar comandos de voz y apareamientos con otros dispositivos teléfonos y blue-Ray. A la vista de muchos esta tecnología sería inteligente pero desafortunadamente no lo es porque entre las vulnerabilidades de seguridad que se encuentran están acceso de datos potenciales sensibles, archivos remotos de información, imagen, o tener acceso total del root.

A través de Scripts y con tarjeta aldrino y los exploits, estos dispositivos manejan autenticación de Null MAC por tal razón todo dispositivo con Null MAC cualquier atacante puede acceder al dispositivo, permite la instalación de Malware mediante las API como File.Unzip o Skipe los hackers los utilizan para copiar archivos objetivos, a su vez los ataque de Man in Madre hace interceptaciones de los datos y comprueba si existen certificados si existen los falsifica, como para esta tecnología no existe antivirus se pueden hacer suplantaciones de sistema operativo de esta forma se hace más fácil el acceso a este tipo de dispositivos.³⁵

³⁵ VULNERABILIDADES DE SEGURIDAD EN SMART TVS Y LAS CONSECUENCIAS EN SU PRIVACIDAD {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <https://www.xataka.com/televisores/vulnerabilidades-de-seguridad-en-smarttvs-y-las-consecuencias-en-tu-privacidad>

8.3. CAPITULO II ATAQUES, ERRORES Y MEDIDAS DE SEGURIDAD EN LOS SMART TV

Partiendo de la página ocho consejos esenciales ³⁶ Es fácil pensar en que el hecho de hacer uso de los dispositivos Smart TV en la sociedad actual va orientado al uso exclusivo de información, el solo hecho de hacer uso de datos hace que esta se exponga y se vulnere, actualmente lo usuarios solo tienen visión de uso, navegación, diversión y no existen advertencias de lo delicado que es navegar sin protección o algún tipo de medida para salvaguardar la misma. Debido a que los Smart TV ofrece características que no son convencionales para los usuarios y con el solo hecho de que no es un dispositivo trasportable que va en los bolsillos, existe un control físico para lo cual los atacantes se les han hecho difícil su violación. Al hacer uso de funciones como contenido multimedia privado, redes sociales y correo electrónico, presenta aspectos vulnerables como información confidencial la cual el usuario no la protege o simplemente la pasa desapercibida, muchos usuarios no utilizan normas de seguridad como claves de acceso o patrones que inicialmente son los más conveniente y fáciles de usar, esto trae consigo que las amenazas este a la vanguardia. La contraseña es, la mayoría de los casos, el único medio o herramienta de seguridad en la mayoría de los Smart TV, La seguridad en los Smart TV depende mucho de la seguridad y la confiabilidad de las aplicaciones que estén disponibles para instalar.

³⁶ OCHO CONSEJOS ESENCIALES PARA EVITAR UN CIBERATAQUE EN TU ORDENADOR {En línea}. {Citado el 21 de Abril de 2018} Disponible en: https://www.huffingtonpost.es/2017/05/12/consejos-para-evitar-un-ciberataque_a_22083669/

Se debe tener en cuenta que los métodos cifrados, permitirán que si existen futuros robos de dispositivo este no permita el acceso a la información, se recalca tener en cuenta esto, se preguntaran es extremo que el TV se pierda, pero existe la posibilidad, es de vital importancia debido a que existen empresas en las que se unen las políticas de seguridad para el uso de estos dispositivos, así que mantener la información asegurada fundamental.

La seguridad de los Smart TV encierra desde SO hasta en el modelo distribución cada una de sus aplicaciones, permitiendo que cada uno de los entornos de desarrollos que existentes de cada plataforma, pueda verlo solo desde el punto de vista del usuario que tiene en funcionamiento el Smart TV.

8.3.1. Ataques más comunes a los dispositivos Smart TV

Técnicas de Haceos y Craqueo Los ataques están diseñados bajo lenguajes como JavaScript o HTML5, los televisores no están optimizados en cuanto a medidas de seguridad. Es sabido que su conexión a la red de internet es por medio de Ethernet o wifi, esta tecnología utiliza chips para poder hacer reproducción de video, pantallas múltiples y hacer conexiones a la red, aparte que hacen uso de una memoria para el procesamiento de los procesos como controlar comandos de voz y apareamientos con otros dispositivos teléfonos y blue-Ray. A la vista de muchos esta tecnología sería inteligente pero desafortunadamente no lo es porque entre las vulnerabilidades de seguridad que se encuentran están acceso de datos potenciales sensibles, archivos remotos de información, imagen, o tener acceso total del root, como se describe adelante.

A través de Scripts y con tarjeta arduino y los exploits, estos dispositivos manejan autenticación de Null MAC por tal razón todo dispositivo con Null MAC cualquier atacante puede acceder al dispositivo, permite la instalación de Malware mediante las API como File.Unzip o Skipe los hackers los utilizan para copiar archivos, a su vez los ataque de Man-in-Middle hace interceptaciones de los datos y comprueba si existen certificados si existen los falsifica, como para esta tecnología no existe

antivirus se pueden hacer suplantaciones de sistema operativo de esta forma se hace más fácil el acceso a este tipo de dispositivos ³⁷.

Ataques en Masa Las aplicaciones interactivas funcionan en diferentes sistemas operativos y podrían permitir ataques de modo que no se tenga mucha experiencia en ataques, las transmisiones falsas podrían robar usuario y contraseña de acceso a redes sociales como Facebook y Yelp, al mismo tiempo que hacen la captura y robo del tráfico de redes Wifi que no se encuentran protegidas.

En los Smarhub (plataforma que permite, navegar por la web, descargar aplicaciones y hacer conexiones con familiares y amigos a través de los servicios que ofrecen las redes sociales), esta podría ser explotada por el usuario local o remoto, activa la webcam y espía a la víctima con una imagen o con sonido.

Los DNS (servicios de nombre de dominio, controlan la configuración de correo electrónico y sitios web del nombre de dominio).³⁸

Muestra como las vulnerabilidades pueden ser combinadas para conseguir historial de búsqueda, cache, cookies, contraseña inalámbrica entre otros. Una

³⁷ TECNICAS DE HACKEO QUE AMENAZAN TU SEGURIDAD {En línea}. {Citado el 21 de Abril de 2018} Disponible en: [https:// platzi.com/blog/tecnicas-de-hackeo/](https://platzi.com/blog/tecnicas-de-hackeo/)

³⁸ LOS ATAQUES INFORMATICOS MAS PELIGROSOS PARA EL BOLSILLO {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <http://www.portafolio.co/tendencias/ataques-informaticos-peligrosos-bolsillo-147718>

particularidad es que utilizan la aplicación esqui que viene integrada en los Smart TV, para inyectar JavaScript malicioso en formato de mensaje forzando el reinicio de la aplicación accediendo a datos almacenados de los usuarios.

DVB-T (Digital Video Broadcasting – Terrestre, estándar de transmisión que se encuentra presente en todos los terminales con conexión a internet), parte de dos vulnerabilidades, conexión a la tv a través de las interfaces web y tomar control del dispositivo, cuando el dispositivo se encuentra comprometido, este puede ser infectado permitiendo así que ningún reinicio de fábrica repare la terminal.

Infecciones por Ransomware (programa dañino que restringe el acceso a determinadas parte de archivos del sistema que se infecta, al mismo tiempo que pide rescate para quitar la restricción), esta infección utiliza métodos de encriptamiento para la información almacenada en los Smart TV, este programa es malintencionado puede llegar en el momento que se encienda la TV se bloquea el equipo en forma total, equipo secuestrado a cambio de dinero, la infección se puede adquirir al momento de descargar aplicaciones para visualizar películas, como se menciona anteriormente se bloquea el sistema y aparece un mensaje donde se indica que hay que realizar un pago para recuperar el dispositivo ya que se ha infringido la ley al momento de la descarga de la aplicación, fraude que asusta a los usuarios y muchos de ellos han realizado el pago para recuperar el control del

dispositivo, aunque el usuario haya intentado restaurar los valores de fábrica del dispositivo ³⁹.

Usuarios: La adquisición de esta tecnología ha venido en aumento los últimos años, el escenario que comparte actualmente capta la atención de los usuarios, el Smart TV es uno de los dispositivos como mayor potencial de crecimiento en los hogares. ¿Porque eligen los usuarios esta tecnología? Con un 84% de su uso en los hogares de Colombia similar a la adquisición de la telefonía de los Smartphone con un 99%⁴⁰.

Poniendo el foco en el uso del Smart TV, casi la totalidad de los usuarios (99%) lo utilizan para mirar películas (83%), series (76%) y noticieros (59%), principalmente a través de Netflix (81%) y YouTube (76%), las plataformas más elegidas por la mayoría de quienes tienen este aparato en su hogar. También se usa para mirar TV tradicional (65%) y escuchar música (58%). Navegar por Internet y mirar fotos son actividades que aparecen en un segundo orden, pero no es de desmeritar, mencionadas por 6 de cada 10 entrevistados. Asimismo, la gran mayoría de los consultados (83%) prefiere elegir contenidos a la carta por tipo y horario, antes que depender de un operador que determine la programación.

³⁹ LOS ATAQUES INFORMATICOS MAS PELIGROSOS PARA EL BOLSILLO {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <http://www.portafolio.co/tendencias/ataques-informaticos-peligrosos-bolsillo-147718>

⁴⁰ LG {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <http://www.lg.com/ar/prensa-y-medios-de-comunicacion/comunicados-de-prensa/lgsmartvmasusado>

Un dato interesante que se desprende del estudio es que 4 de cada 10 entrevistados declaran no usar sus Smart TV con señal de cable (39%). No obstante, el uso con cable asciende al 61%, duplicando al uso del dispositivo con Internet (31%) y triplicando la conexión satelital (17%). La principal razón de mantención del cable es que los actuales proveedores permiten contratar paquetes con otros servicios (internet, telefonía): 4 de cada 10 así lo indican. En menor medida se alude a que no existe diferencial de precio con otras opciones del mercado (19%), seguido de cerca por el hecho de no tener un Smart TV que justifique la baja (17%). Ante la eventual falta de cable, 3 de cada 10 personas consultadas optarían por señal satelital o Internet (29%), aumentando significativamente en el interior del país (33%).

Reiterando el Smart TV, brinda de posibilidades de entretenimiento que son numerosas. El fácil uso la conexión sencilla permite hacer una navegación en red de forma entretenida, ingresar a redes sociales, descargar cientos de aplicaciones y juegos, visualizar películas y series en streaming, escuchar música y poder disfrutar de miles de contenidos en la mejor de las definiciones ⁴¹.

⁴¹ LG {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <http://www.lg.com/ar/prensa-y-medios-de-comunicacion/comunicados-de-prensa/lgsmartvmasusado>

8.3.2. Errores de los usuarios

No cerrar las sesiones adecuadamente: cada vez que se haga uso del correo electrónico se debe asegurar de cerrar la sesión ⁴².

Diferentes personas hacen que sus dispositivos electrónicos que están a su disposición como Smart TV, teléfonos tabletas los hagan medios, que ofrecen servicio de internet, hay que tener en cuenta que las sesiones abiertas en diferentes sitios se deben cerrar y asegurarse que al abrir de nuevo la página no se direcciona a algún formulario de datos personales.

No borrar el caché, el historial y las contraseñas: muchos de los navegadores web recopila automáticamente las direcciones donde se accede. La recomendación más segura es tratar de borrar todos los registros y no aceptar guardar contraseñas en estos. Teniendo en cuenta el sitio web IT Security, esta información puede usarse para hacer suplantaciones de identidades y hacer estafas bancarias.

Pensar que todos los correos electrónicos son verdaderos: Los correos electrónicos que contengan firma electrónica de alguna empresa, no están exentos de que sean 100% seguros que sea real, esta práctica es popular entre los

⁴² SI, TU SMART TV TE ESPIA – PERO SOLO SI LOS PERMITES {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <https://es.gizmodo.com/si-tu-smarttv-te-espia-pero-solo-si-se-lo-permites-1684643092>

ciberdelincuentes y su nombre es phishing, engañar al usuario solicitando cambiar su contraseña personal de transacciones seguido re direccionándolo al usuario a un sitio web falso, donde probablemente se hará captura y robo de los datos personales. Es correcto e inmediato eliminar de la bandeja todo correo que desconozcamos su destinatario, sin hacer clic en alguna de sus opciones o archivos adjuntos. Hay que tener en cuenta la presencia de estos correos en la bandeja de entrada:

- Teniendo en cuenta el artículo si, tu Smart TV te espía- pero solo si lo permites. Ninguna entidad bancaria le pedirá cambio de password en un email.
- Singularmente usan 'Apreciado usuario' o 'Apreciado cliente', en cambio de su nombre original
- Algunos contienen amenazas de acciones legales o anuncios atemorizantes, sin mayores datos adicionales.
- La dirección electrónica del correo no usa la URL de la entidad bancaria.
- Siempre exigen acciones inmediatas.

Compartir sus contraseñas con otras personas: tener cierto grado de confianza con un compañero o amigo no significa que sea necesario divulgar tu información personal o contraseñas, se debe tener en cuenta que estas son únicas e intransferibles independiente de la persona que se, hay que ser.

- Si tiene su antivirus actualizado
- Si no lo va a compartir con otras personas
- Si la otra persona accede desde un equipo o una red que no es segura.
- Si no va a intentar entrar a sus redes sociales con la misma clave.

Usar la misma contraseña en todas sus cuentas: tener una mala memoria para las contraseñas a la hora de hacer uso de los diferentes sitios electrónicos es una falta grave. Es tal vez una de las causas principales de vulnerabilidad de la información, utilizar exclusivamente el mismo password en los servicios electrónico. Si alguna persona accede o roba esa contraseña tendrá prioridad para entrar a sus redes sociales, correo electrónico, su información bancaria y en sus cuentas en sitios de comercio electrónico.

Aunque parezca cansón, hay que ser precavido y manejar distintas claves para cada uno de los sitios accesibles en internet. Esto incluye las contraseñas que utiliza para acceder a las conexiones inalámbricas de su hogar u oficina.

Pensar que todas las conexiones gratuitas son seguras: Lugares públicos como aeropuertos y hoteles, entre sus servicios permiten de conectarse de forma gratuita a redes inalámbricas. Hay que tener en cuenta, que estas conexiones casi siempre no son seguras, el administrador de la red puede acceder a datos de los equipos que se conectan o descifrar las contraseñas de los dispositivos. Absténgase de

hacer uso de redes de internet públicas, cuando deba realizar tareas confidenciales o que impliquen entregar datos sensibles, use sus redes personales.

Revelar más información de la necesaria: Las páginas donde las personas comparten contenido personal Facebook, Twitter, Instagram entre otras, desde su nacimiento han dado un vuelco total a los usuarios, se convirtieron verdaderos productores de contenido, en los cuales comparten usualmente imágenes, video, opiniones y comentarios. Es allí donde la mayoría de las personas comparten datos personales en línea sin pensar cuales son las implicaciones que esto puede traer. “La mayoría de las personas no cran hábitos seguros y su pensamiento solo se dirige a subir y a subir información, se debe tener en cuenta lo siguiente.

- Cuando la información se encuentre en línea, a merced de cualquier otro usuario, este pierde control absoluto sobre la información.
- Los datos no saben quién los administra, y se ha llegado a saber hasta conocer el día y el lugar de nacimiento de sus víctimas puede ser muy valioso para un pirata digital.

Mejorar la Navegación: Según la página consejos para mejoras la navegación por internet ⁴³, cable Ethernet: tener en cuenta la calidad de la conexión la cual

⁴³ CONSEJOS PARA MEJORAR LA NAVEGACION POR INTERNET EN LOS SMART TV {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <https://larepublica.pe/tecnologia/811758-6-consejos-para-mejorar-la-navegacion-por-internet>

determina si los usuarios pueden disfrutar al máximo las aplicaciones como Netflix y los servicios alternos que ofrece con resoluciones full HD o 4K. La principal recomendación es conectar el Smart TV directamente a internet mediante un cable Ethernet, conectar un cable al TV desde el modem asegura que la señal no sufra perdidas y que se vea menos vulnerable a ataques. Conexión: al momento de conectar el Smart TV a la red wifi se debe tener en cuenta que la conexión cuente con una transmisión mínima de 15 MB por segundo para evitar problemas ⁵⁵.

Actualizaciones

Tener en cuenta el tipo de actualizaciones para el software que ofrece la tv.

- Desconfiar de las actualizaciones desconocidas o no oficiales
- No realizar pagos online a través de tu Smart TV, y asimismo, evitar introducir datos personales.
- Si el Smart TV posee web Cam, cúbreala siempre que no se esté utilizando.
- Actualizar el firmware o programa que usa el televisor para parchar fallas de seguridad.
- No dejar claves por defecto que vienen en los Smart TV.
- No activar servicios de anuncios, bloquearlos todo servicio o app instalada puede estar recopilando distintos datos

Usa apps de confianza: Se debe tener en cuenta que un Smart TV es un poseedor de gran cantidad de aplicaciones, hacer uso de ellas en la pantalla del dispositivo.

Para tener en cuenta ¿qué sucede si atacan una de estas apps sin que te des cuenta? Es preciso descargar aplicaciones que se conocen y son confiables. Posiblemente.

8.3.3. Aplicaciones seguras para los Smart TV

Las APPS para Smart TV manejan una arquitectura semejante a la de las páginas web. Los diccionarios de JavaScript permiten consultar y visualizar los contenidos como álbumes, archivos css que mejoren el estilo de la aplicación y las interfaces ya que es la capa final de los resultados previstos. Seguido se hará una descripción de alguna de las aplicaciones más usadas y que brindan seguridad de la transmisión de los datos a la hora de hacer uso del dispositivo.

Gaia: una plataforma de seguridad que está presente en los Smart TV con Tizen, basado a su vez en Linux, seguro, permite que las actualizaciones de las aplicaciones de los dispositivos, esta establece tres capas de seguridad al estar integrado el núcleo, protegiendo así los datos de forma más eficiente. GAIA se encargará de proteger bajo un PIN las credenciales de acceso del usuario a los diferentes servicios, así como datos bancarios que se utilicen en el equipo. La segunda capa está relacionada con los protocolos de transporte de la información y el envío de la misma, estableciendo un canal robusto sobre el que la información se enviará cifrada. Para terminar, la tercera podría considerarse como una sandbox,

permitiendo a Tizen ejecutar aplicaciones sin que estas tengan la potestad de realizar cambios importantes en el dispositivo ⁴⁴.

Safe Browsing es una capa de seguridad similar a un antivirus, usa como base los motores de seguridad de Google para hacer la protección en tiempo real, de amenazas que pueden llegar al navegador, ya sea descarga de virus o re direccionamiento a páginas web que puedan ser peligrosas, este módulo de seguridad se incluye por defecto en Google Chrome, el cual por defecto viene instalado en nuestros dispositivos Smart TV.

Aplicaciones Web o Web Apps: generalmente utilizan una función Web View, a la hora de ejecutar una aplicación independiente se carga el motor web para hacer conexión a una web optimizada viéndose dentro de la aplicación, estas aplicaciones no se ejecutan dentro del navegador, solo están disponibles si los desarrolladores programan e implementen esta característica manual, algo que todavía no es muy usual.

Windows Defender: es un antivirus gratuito, integrado a la mayoría de los sistemas operativo de los Smart TV, con una excelente tasa de detección frente a las amenazas, incluso para las que a diario se crean. Además, es un motor antivirus

⁴⁴ 7 APLICACIONES PARA TU TELEVISOR SMART TV {En línea}. {Citado el 21 de Abril de 2018} Disponible en: <http://www.samsung.com/es/a-fondo/contenidos-y-servicios/7-aplicaciones-para-tu-televisor-samsung-smart-tv/>

que mejor protección ofrecen frente a los ataques informáticos basados en el navegador, como es el phishing.

Eset Smart TV Security: solución a la seguridad con tecnología avanzada contra ataques de Malware dirigidos a los Smart TV, teniendo en cuenta las estadísticas en donde 30 billones de dispositivos conectados a internet, el hecho de reiterar el uso de micrófonos, cámaras, puertos USB, son objetivo principal para los malware permitiendo así control sobre el dispositivo, al mismo tiempo el espionaje de usuarios que podrían proporcionar información sensible. Eset Smart TV Security ofrecen la siguiente funcionalidad:

- Antivirus, brinda seguridad ante niveles crecientes de Malware.
- Es una tecnología anti-Ransomware combatiendo los bloqueos de pantallas.
- Multi-device scanning para malware en memorias usb que se conectan a los Smart TV.
- Anti-Phishing protección a los usuarios de intentos de robo de información personal sensible.

Pasando de la página aplicaciones para tu televisor, **Android Market** Una de las principales características de Google es que no existe límite en el número de compartir Apps. Existen reglas para Google pero a la hora de hacer uso de la App la responsabilidad plena de uso es únicamente del usuario. La protección del dispositivo ante ataques tiene que ver con las capacidades que incluya cada

programa dentro de sus funcionalidades. En cuanto se instale una aplicación Adroid, el sistema operativo tendrá la función de hacer una lista de los requerimientos para esta la cual permitirá su ejecución, como se mencionó inicialmente es de suma importancia que el usuario tenga conciencia de su funcionalidad para prevenir posibles vulnerabilidades. Teniendo en cuenta otros aspectos Google con algún tipo de código malicioso tendrá la capacidad de deshabilitar de forma remota estas características, de igual forma cuando el dispositivo Smart TV requiera interactuar con aplicaciones, deberá solicitar permisos requeridos para lo cual los desarrolladores hayan declarado para estas.

29 Consejo Nacional Consultivo de Cyber – Seguridad. Malware en Smartphones. En: Mercados de aplicaciones. P.15-16.

Lookout security suite protección anti-virus, una de sus características principales es (contactos, fotos, video, correo electrónico y mensajes de texto), además contiene un localizador para dispositivos, este se puede usar para mostrar la ubicación del dispositivo en un mapa online, al igual da opción de eliminar de forma remota todos los datos en el dispositivo por x razón. Estas funcionales se pueden usar de forma remota desde la interfaz basada en Web. Lookout parece ser la opción más completa

Gestionar todas las contraseñas LastPass aplicación de Android con el navegador de Firefox para PC, Safari, Chrome e Internet Explorer. Permite que las contraseñas maestras de acceso a sitios en la nube, genere contraseñas de forma

automática periódicamente o cuando el sistema lo requiera, en el navegador del Smart TV como en la nube. Tiene la capacidad de gestionar contraseñas y almacenarlas, tarjetas de crédito, PINs, protegidos con cifrado Blowfish de 256 bits. Opcionalmente se puede utilizar para sincronizar datos del celular con una PC, Smart TV.

8.4. CAPITULO III CARACTERISTICAS DE LA SEGURIDAD DE LOS SISTEMAS OPERATIVOS USADOS EN LOS SMART TV

Android TV Es uno de los Sistemas Operativos más populares actualmente, familiar para las experiencias de los usuarios, similar a la de los Smartphone y tables inclusive se pueden utilizar las mismas aplicaciones. Google Play es una herramienta que permite la descarga e instalación de las aplicaciones que necesiten los usuarios, el navegador utilizado por estos dispositivos es Chromecast brinda la posibilidad de navegación y visualización de contenido de internet. De igual forma permite la conexión de periféricos como teclados para suprimir complicaciones a la hora de hacer uso del control mágico, rápido y sencillo.

Reiterando que este dispositivo tiene acceso a una serie de servicios a los que una TV normal no tiene acceso, conlleva a riesgos, este Sistema Operativo ofrece una VPN (Red privada virtual que permite una extensión segura de la red de área local, sobre una red pública o no controlada como Internet), la cual se instala en el Android TV, permite el cifrado de la conexión a internet mejorando la privacidad y seguridad online en el Smart TV, al momento que el dispositivo esté conectado a internet, la

privacidad puede estar en riesgo, esto incluye Hackers o fisgones de actividades, o que su ISP proveedor de servicios recoja información sobre las actividades y comportamientos del dispositivo. Al momento de usar la VPN la conexión del Smart TV estará mucho más protegida mejorando la privacidad del televisor, a su vez mejora la experiencia de Streaming con velocidad de contenidos y termina con las limitaciones de los ISP.

Linux: Su objetivo principal es la utilización de la redes y funciones multiusuario, se explican algunas de sus importantes ventajas. Únicamente los usuarios administradores pueden hacer diferentes cosas en el Sistema Operativo.

Un ejemplo es no se permite archivos ejecutables en el registro, teniendo en cuenta que a los mismos se le den permisos y permitan el desarrollo o instalación de la aplicación. Este Sistema Operativo hace uso de archivos que configuran los registro de las actividades independientemente esto quiere decir que; se configura de forma individual, dentro de sus medidas de seguridad se destaca la descentralización de datos que evita la creación de bases de datos a su vez elimina y detecta programa maliciosos, así como dificulta su reproducción basándose en las facultades del administrador que puede hacer edición de archivos del sistema.

Se destacan y recomiendan algunas herramientas base para la seguridad de la información. Este sistema operativo dentro de su prototipo presenta un diseño modular el cual elimina un módulo cualquiera del sistema en caso de ser necesario, hay que tener en cuenta que Linux es el Kernel de los Sistemas Operativos al cual no se le permite acceder de forma directa pero dentro de su distribución existe una interfaz grafica la cual se compone de un numero de herramientas que gestionan

las ventanas, logins, otro encargado del sonido, otro del video y otro de proyectar el panel del escritorio, cada módulo conforma su interfaz gráfica la cual se utiliza a diarios. Repositorios y Software la mayoría de los usuarios tiende a descargar aplicaciones con crack licencias que permiten su funcionamiento libre sin remuneración económica, la mayoría de estos contienen virus o malware, este Sistema operativo permite la instalación de software libre.

Tizen Os: Este sistema operativo es líder de la marca Samsung y no tiene buenas referencias de seguridad tanto que se atrevieron a asegurar que “todo lo que hicieron mal lo hicieron, es bastante obvio que nadie con la más mínima comprensión sobre temas de seguridad informática miro y escribió este código. Es como si hubieran puesto a un estudiante a programar su software”. Los dispositivos Smart TV con sistema operativo Tizen Os son vulnerables y no solo estos a su vez los relojes inteligentes y los smartphones, son susceptibles a ser intervenidos y se demostró más de 27.000 errores delicados en su sistema que ponen en riesgo la información. Dentro de las novedades negativas esta que es un nido de Malware donde siembra el caos en internet, a su vez que permite que cualquier hacker ejecute código de forma remota para tener acceso remoto del dispositivo. Tan a la ligera parece haberse escrito su código que hasta la tienda de aplicaciones.⁴⁵

⁴⁵ QUE SISTEMA OPERATIVO PARA SMART TV ME CONVIENE MÁS {En línea}. {Citado el 21 de Abril de 2018} Disponible en http://www.parentesis.com/tutoriales/Sistemas_operativos_mas_populares_para_Smart_TVs

Tizen Os tiene privilegios para hacer y deshacer en el sistema a su antojo, una entrada para las aplicaciones que contengan código malicioso, la marca que utiliza este sistema operativo hace caso omiso a estas investigaciones que perjudican a los usuarios que hacen uso de este sistema operativo es sus dispositivos en este caso los Smart TV.

Parece que parecieran insignificantes las advertencias, esta investigación preocupa si se tienen en cuenta que Samsung, en su objetivo de reducir la dependencia con Android, ha instalado Tizen en 30 millones de Smart TV.

Web OS: considerado uno de los mejores sistemas operativos para Smart TV implementado por la marca LG, su funcionalidad Security Manager se ha certificado por sus **capacidades de ciberseguridad**, teniendo en cuenta el test UL 2900-1 mide la seguridad de las aplicaciones y el acceso a la información a través de procesos de autenticación, protección contra hackeo y protección contra la falsificación de software, es la primera plataforma en conseguir certificación UL 2900-1, funcionalidades de gestión de los derechos digitales de las “apps” de los Smart TV, este programa a testado en la funcionabilidad de Security Manager para comprobar sus vulnerabilidades, susceptibilidad de Malware, debilidades de software y controles de seguridad que ayudan a proteger la información privada de los usuarios.

Esta plataforma es desarrollada en base a la seguridad UL evoluciona, se somete a gran cantidad de ataques virtuales a la red, o asaltos a la vulnerabilidad, ejemplo ataques al top 25 CWE/SANS aplicaciones del centro de seguridad del sistema, esta plataforma es muy intuitiva. Supone que esto es un hito en la industria ya que son los primeros televisores en obtener esta certificación dentro de la categoría de Smart TV, aunque se debe de tener en cuenta que los sistemas de seguridad contra ataques no son 100% seguros, la marca LG pone todos sus esfuerzos en tratar de impedirlo a toda costa aumentando su nivel de seguridad de muchos de sus productos, este caso sus televisores y dentro de sus resultados esta la obtención de su certificado UL que lo designan una de las empresas más importantes de seguridad informática del mundo, concretamente el test UL 2900-1 mide procesos de autenticación, protección contra Phishing y falsificación de software así como su nivel de protección contra distintos tipos de Hackeos. El test comprueba si la aplicación es totalmente segura ante cualquier amenaza poniéndola a prueba mediante diversos procesos. LG con WEB OS 3.5 una versión del Sistema Operativo, a su vez se certifica en aptitudes a la hora de gestionar los derechos digitales de las Apps de los Smart TV. Teniendo en cuenta la meta de cumplir con este estándar, sirve de partida para las redes IoT compuestas por diferentes aparatos de nuestro hogar, conexión de electrodomésticos.

Otras características tenidas en cuenta para la seguridad de los dispositivos ofrece un sin número de contenidos en los Smart TV, es intuitivo y practico de forma impresionante su interfaz es muy similar a la de un dispositivo móvil celular. Teniendo en cuenta el artículo de la página LG LGTV.cl "La seguridad del sistema

ha sido certificada por **UL Cybersecurity Assurance Program (CAP2900-1)**, por lo que vivirás una experiencia de TV en la que puedes confiar en un 100%. El sistema webOS 3.5 te protege de aplicaciones que no están autorizadas, de hackeo y de violaciones de privacidad (en este post te contamos todos los detalles del nuevo sistema de seguridad de webOS)". Otra razón de seguridad de iOS es que una aplicación no puede buscar, ver o modificar códigos o datos de las demás, estas aplicaciones no tienen acceso raíz al núcleo o a los recursos sensibles del dispositivo. Todas las aplicaciones operan con los mismos permisos de baja granularidad, salvo unas pocas excepciones controladas por los usuarios, como el acceso a la ubicación y las notificaciones.

iOS hace más difícil el abuso por parte de aplicaciones maliciosas o pobremente escritas, aunque presenta un mínimo de vulnerabilidad, los ataques via navegador están presentes. Ejemplo, las aplicaciones de iOS descargadas mediante jailbreak usan bugs en el navegador Safari. Cosa que los escáneres antimalware no detectan este tipo de actuaciones, de igual manera soportan de forma nativa los controles de seguridad normalmente exigidos por las empresas, incluyendo el control de acceso a nivel de dispositivos, bloqueo/limpieza remotos y encriptación de la información en reposo y en tránsito. Pueden requerir usar un PIN o contraseña de complejidad específica, auto bloquear la pantalla del dispositivo después de un periodo de inactividad o bloquear remotamente el dispositivo conectado a la red. Usa encriptación para proteger los datos en reposo, pero las capacidades del hardware varían de modelo a modelo.

9. CONCLUSIONES

- Durante el desarrollo de la presente monografía se realizó análisis del estado actual de la seguridad informática en los dispositivos Smart TV y la forma de como los usuarios hacen uso de la misma, fortaleció el conocimiento y brindo un diagnostico general sobre la importancia tomar las medidas de seguridad para proteger la información
- Se identificó los antecedentes de la evolución de la televisión y el cambio de estado de una televisión convencional a una televisión interactiva, contextualizando un análisis de cómo se encuentra actualmente la seguridad informática de estos dispositivos, arquitectura, diseño de software y las aplicaciones más convencionales para generar protección de la información.
- La base del Malware radica en la descarga de aplicaciones no conocidas a través de la aplicación App Store, no obstante, se tuvo presente que gran parte de los usuarios de Smart TV no hacen uso de antivirus en este tipo de dispositivos.
- Los dispositivos Smart TV son cada vez más vulnerables a los ataques de Wi-Fi, teniendo en cuenta que las mismas aplicaciones dan paso a que los

atacantes acceder fácilmente al correo electrónico de la víctima y a las aplicaciones de redes sociales.

- Conductas de riesgo de desconocimiento. El factor ignorancia y desconocimiento de seguridad de la información hace que los datos se expongan y se violen dando paso a que personas y organizaciones, pierdan tiempo y dinero.
- Se presentaron algunas medidas para proteger el activo de la información teniendo en cuenta que los ataques informáticos no disminuyen por el contrario aumentan y son capaces de exponer los datos a actividades indebidas que no requieran de su uso, hay que estar siempre a la vanguardia de la tecnología en cuanto a seguridad de la información, siempre se debe tener en cuenta la importancia de tener conocimiento, técnicas, indagar sobre cómo proteger los datos capacitarse y sensibilizarse en cuanto la seguridad de los dispositivos así como también no olvidar la seguridad física y del entorno y aplicar los controles necesarios.

BIBLIOGRAFIA

Alex Aliaga. 12 de Marzo de 2010. Android en un microondas, {En línea}, {29 de mayo de 2018} Disponible en internet en: <http://www.linuxzone.es/2010/03/12/android-enun-microondas/>

Futuro de la seguridad en el Hogar, David Camilo Parra Arias, Manuel Fernando Ramírez Chaparro {En línea}, {26 de Agosto de 2018} disponible en: <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2902/00001359.pdf?sequence=1>

Hackear una Smart TV remotamente. {17 de Agosto de 2018} disponible en: <https://ciberseguridad.blog/hackear-una-smart-tv-remotamente/>

Haking, surveilling, and deceiving victims on Smart TV “Allanar, vigilar y engañar a las víctimas en Smart TV” {En línea}, {26 de mayo de 2018} disponible en: <https://txt.731my.com/tmp/blackHat/US-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf>

Interacción Humana con los Ordenadores, Usabilidad en dispositivos Smart TV: {En línea}, {29 de mayo de 2018} disponible en: openaccess.uoc.edu/webapps/o2/bitstream/10609/18529/3/jnietoruTFC0113memoria.pdf

Monografía Características y parámetros de la seguridad para los Smartphone con sistema Operativo Android” {En línea}, {29 de mayo de 2018} disponible en: <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2519/?sequence=4>

Nos pueden espiar desde nuestro Smart TV. {En línea}, {26 de mayo de 2018} disponible en: <https://www.seas.es/blog/informatica/nos-pueden-espiar-desde->

nuestra-smart-tv/

Peligro Para los Smart TV: una vulnerabilidad permitirá ataques en masa {En línea}, {28 de mayo de 2018} disponible en: <http://www.globalgate.com.ar/novedades-peligro-para-los-smart-tv-una-vulnerabilidad-permitiria-ataques-en-masa.html>

Smart TV Haking {En línea}, {17 de Agosto de 2018} disponible en: <http://www.delaat.net/rp/2012-2013/p39/report.pdf>

Samsung Electrónicos: “E-Manual”. {En línea}, {29 de mayo de 2018} disponible en: [http://downloadcenter.samsung.com/content/UM/201304/20130413105554609/\[SPA\]FPDVEUF-1.004-0401.pdf](http://downloadcenter.samsung.com/content/UM/201304/20130413105554609/[SPA]FPDVEUF-1.004-0401.pdf).

Smart TV Alliance: “Smart TV Alliance SDK Documentation”. {En línea}, {29 de mayo de 2018} disponible en: <https://developers.smarttv-alliance.org/sdk-documentation>.

Secure communication in Digital TV Broadcasting “comunicación segura en la difusión de televisión digital”: {En línea}, {29 de Agosto de 2018} disponible en: <https://pdfs.semanticscholar.org/cc7a/43ebdc06b27a4bf6e2472bae4cda0321c627.pdf>.

Tecnología & Informática, vulnerabilidades informáticas {En línea}, {25 de mayo de 2018} disponible en: <https://tecnologia-informatica.com/vulnerabilidades-informaticas/>

TECNOLOGIA, Que es Smart TV Características, {En línea}, {25 de mayo de 2018} disponible en: <http://www.areatecnologia.com/que-es-smart-tv.htm>

Vulnerabilidades de seguridad en Smart TV y las Consecuencias en tu privacidad {En línea}, {25 de mayo de 2018} disponible en: <https://www.xataka.com/televisores/vulnerabilidades-de-seguridad-en-smarttvs-y-las-consecuencias-en-tu-privacidad>

ANEXOS

Anexo A Formato RAE

TEMA	Diseñar una monografía para la gestión de la seguridad de la información de los usuarios que hacen usos de los dispositivos Smart TV.
TÍTULO	Características y parámetros de la seguridad en la transmisión de datos para los dispositivos Smart tv.
AUTORES	Johana Rocio Rojas Camacho
FUENTES BIBLIOGRÁFICAS	<p>Se referencia 9 fuentes bibliográficas, algunas que mencionan la temática principal son: Alcaldía de Bogotá. Acuerdo 514 de 2012, diciembre 18. Disponible en:</p> <p>Vulnerabilidades de seguridad en Smart TV y las Consecuencias en tu privacidad {En línea}, {25 de mayo de 2016} disponible en: https://www.xataka.com/televisores/vulnerabilidades-de-seguridad-en-smarttvs-y-las-consecuencias-en-tu-privacidad.</p> <p>Televisión Inteligente {En línea}, {26 de mayo de 2016} disponible en: https://es.wikipedia.org/wiki/Televisi%C3%B3n_inteligente.</p> <p>TECNOLOGIA, Que es Smart TV Características, {En línea}, {25 de mayo de 2016} disponible en: http://www.areatecnologia.com/que-es-smart-tv.htm.</p>

	<p>Peligro Para los Smart TV: una vulnerabilidad permitirá ataques en masa {En línea}, {28 de mayo de 2016} disponible en: http://www.globalgate.com.ar/novedades-peligro-para-los-smart-tv-una-vulnerabilidad-permitiria-ataques-en-masa.html.</p> <p>Monografía Características y parámetros de la seguridad para los Smartphone con sistema Operativo Android” {En línea}, {29 de mayo de 2016} disponible en: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2519/?sequence=4.</p>
AÑO	2018
RESUMEN	<p>La presente Monografía quiere promover la seguridad de las nuevas tecnologías en este caso los dispositivos Smart TV, es una propuesta la cual aborda el tema seguridad de la información en dispositivos que captan la atención de la mayoría de los usuarios que hacen uso de este dispositivo. Describe básicamente el condicionamiento de la forma de vida y la conectividad casi que las 24 horas del día a la internet, permitiendo así que el usuario este hiperconectado mediante una pantalla, esta crea dependencia por la variedad de las aplicaciones y novedades que presentan los Sistemas Operativos en este caso Android TV, Tizen, Firefox OS o WebOs, los cuales buscan generar mejores experiencias en su uso.</p>

PALABRAS CLAVES	Smart TV, usuarios, Activo, amenaza, clave pública, contraseña, televisión, seguridad, amenazas, delitos, aplicaciones, Internet, vulnerabilidades, ataques, arquitectura, sistemas operativos, protocolos, errores.
CONTENIDOS	<p>Evolución de la Televisión convencional hasta llegar a un Smart TV.</p> <p>Interconectividad del todo, Dispositivos Smart TV.</p> <p>Ataques dirigidos y ciberspionaje</p> <p>Estrategias de seguridad en los dispositivos Smart Tv</p> <p>Panorama de amenazas a los dispositivos a través de internet</p>
DESCRIPCION DEL PROBLEMA	<p>Actualmente la seguridad informática tiene un papel muy importante en la era tecnológica, la información puede ser encontrada de distintas forma, almacenada electrónicamente, a través de correo electrónico, en videos, grabaciones, o en cualquier medio digital etc. Es así que a través de cualquiera de estos medios la información se puede ver amenazada o vulnerada, a su vez los delitos informáticos han tenido un gran aumento a nivel mundial, la falta de conocimiento sobre cómo deben protegerse y el sin número de técnicas en donde los atacantes consiguen obtener información confidencial, es allí donde se ve la necesidad de derribar algunos mitos y aclarar algunos conceptos sobre la importancia de la</p>

	seguridad de la información al momento de hacer uso de los dispositivos Smart TV.
OBJETIVOS	<p>OBJETIVO GENERAL</p> <p>Desarrollar una monografía que condense las principales características y parámetros de seguridad en transmisión de datos para los Smart TV teniendo en cuenta diferentes Sistemas Operativos.</p> <p>OBJETIVOS ESPECIFICOS</p> <ul style="list-style-type: none"> • Realizar un Análisis de la evolución de los dispositivos Smart TV. • Determinar parámetros y características de seguridad de los 5 sistemas operativos más comunes en los dispositivos Smart TV. • Identificar los errores más comunes que comenten los usuarios durante su uso y herramientas que permitan mejorar la seguridad de la información en dispositivos Smart TV. • Determinar cuáles son los Sistemas Operativos más recomendables que permitan salvaguardar la información en los dispositivos Smart TV.

PRINCIPALES REFERENTES TEÓRICOS	Se utilizan los conceptos básicos referentes a seguridad y metodología que proporcionan herramientas para proteger la información al momento de hacer usos de los dispositivos Smart TV.
PRINCIPALES REFERENTES CONCEPTUALES	Seguridad de la información, objetivos de la seguridad de la información, infraestructura computacional, los usuarios y la información, tipos de vulnerabilidades y su clasificación, amenazas y sus tipos.
RESULTADOS	Concientización de los usuarios de las normas que deben de tener a la hora de hacer usos de estos dispositivos, concientizar a los usuarios que la seguridad de la información no solo es un tema, además es una práctica fundamental, identificación que la falta de conocimiento en técnicas de protección de la información son casi que desconocidas para los usuarios comunes, fortalecimiento de políticas y mecanismos de educación tecnología o manuales de usuario para incentivar la protección de la información
CONCLUSIONES	1. Durante el desarrollo de la presente monografía se realizó análisis del estado actual de la seguridad informática en los dispositivos Smart TV y la forma de como los usuarios hacen uso de la misma, fortaleció y conocimiento y brindo un diagnostico general sobre la importancia y medidas necesarias para proteger el activo al hacer uso de el.

	<p>2. Se identificó los antecedentes de la evolución de la televisión y el cambio de estado de una televisión convencional a una televisión interactiva, contextualizando un análisis de cómo se encuentra actualmente la seguridad informática de estos dispositivos, arquitectura, diseño de software y las aplicaciones más convencionales para generar protección de la información.</p> <p>3. La base del Malware radica en la descarga de aplicaciones no conocidas a través de la aplicación App Store, no obstante, se tuvo presente que gran parte de los usuarios de Smart</p>
--	--